APPENDIX A

Surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA)

Policy and Procedure

September 2022

Document Location

This document is held by Tandridge District Council, and the document owner is the Senior Responsible Officer.

Printed documents may be obsolete. An electronic copy will be available on Tandridge District Council Intranet. Please check for the current version before using.

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and the Council's website.

Date	27th September 2022
Version	V3
Review date	September 2023
Owner	Lidia Harrison – Monitoring Officer

Record of amendments

Amended Month/Year	Version	Details	Amended by
March 2019	V.1		Jason Thomas
September 2020	v.2		Lucinda Capel
September 2022	v.3		Katy Humphrey

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

DEFINITIONS

Unless the context otherwise requires, in this document the expressions in the first column shall have the meaning in the second column and any reference to a statute or statutory instrument or code of practice within the document shall include amendments to it.

Act	means RIPA.
Authorising Officer	RIPA refers to "**Designated Officers**". For ease of understanding and application this document refers to Authorising Officers. These are those posts referred to in Annex A and any that are duly added to or substituted by the Senior Responsible Officer.
CHIS	means Covert Human Intelligence Source.
Council	means Tandridge District Council.
Covert Surveillance	means surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place (Section 26(9) (a) of RIPA). It can be either directed or intrusive.
Directed Surveillance	means surveillance which is covert but not intrusive and which is undertaken for the purpose of a specific investigation or specific operation in such a manner as is likely to result in obtaining private information about an individual (whether or not that person is specifically targeted for purposes of an investigation (section 26(10) of RIPA)). Directed surveillance may only be undertaken in the investigation of a criminal offence attracting a criminal sentence of not less than 6 months imprisonment or the investigation of offences relating to the sale of alcohol or tobacco to children.
Intrusive Surveillance	as defined in section 26(3) of RIPA as covert surveillance that: a) is carried out in relation to anything taking place on any residential premises or in 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.

	Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.
Monitoring Officer	means Lidia Harrison
RIPA	means the Regulation of Investigatory Powers Act 2000.
RIPA Authorising Officer Certificate	means the form in Annex B.
RIPA Co-ordinating Officer	means Katy Humphrey
Senior Responsible Officer	means the Monitoring Officer.
Surveillance	means monitoring, observing or listening to persons, their movements, conversations, other activities or communications, recording anything monitored, observed or listened to in the course of surveillance and surveillance with a surveillance device (which means anything designed or adapted for surveillance use).

1. Introduction

1.1 The Council is committed to improving the quality of life for the communities of the District which includes benefiting from an attractive place to live, meeting the needs of local people and employers with opportunities for all to engage in community life. It also wishes to maintain its position as a low crime district and a safe place to live, work and learn. Although most of the community comply with the law, it may be necessary to carry out enforcement action against those that flout it. Any enforcement action will be conducted in a fair, practical and consistent manner to help promote a thriving local economy.

1.2 There are many reasons why the Council might need to carry out surveillance investigations, for example, investigating anti-social behaviour, fly tipping, nuisance control, planning (contraventions), fraud, licensing and food safety legislation. This list is not intended to be exhaustive. In most cases, Council officers carry out investigations openly and in a way which does not interfere with a person's right to a private life. However, there may be instances where it is necessary for officers to use covert surveillance techniques to undertake a specific investigation.

1.3 As all surveillance is likely to intrude upon someone's human rights, it is important that the Authorising Officer is able to justify that the breach of privacy is necessary, proportionate and lawful. It is also essential that the reasoning is fully documented and the correct authorisations gained (in order that the Council is able to justify its actions if challenged).

1.4 Surveillance therefore plays a necessary part in modern life as a means of detecting criminals and of preventing crime and disorder. Parliament passed RIPA to ensure that public bodies charged with these duties use their investigatory powers in accordance with the Human Rights Act 1998 (**HRA**) and the Data Protection Act 2018 (**DPA**).

1.5 This Policy and Procedure document sets out the means of compliance with, and use of, RIPA by the Council in its capacity as a local authority. It is based upon the requirements of RIPA and the national Codes of Practice issued by the Home Office and the Investigatory Powers Commissioner's Office (**ICPO**). Links to the Home Office Guidance and Codes of Practice can be found here:

RIPA codes - GOV.UK (www.gov.uk)

1.6 The Council's Policy is operational forthwith and applies to all Council staff employed under a permanent, temporary, fixed-term or casual contract. It also applies to any contractors and/or subcontractors employed by the Council. It is also important that the Authorising Officer is aware of the abilities of its operatives to ensure they are capable of undertaking the surveillance.

1.7 If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman and/or the Council could be ordered to pay compensation.

1.8 Members have also a role to play in reviewing the Council's use of RIPA to ensure that it is being used consistently with this Policy. They will also ensure that it is fit for purpose. However, Members will not be involved in making decisions on individual authorisations.

1.9 The authoritative position on RIPA is, of course, the Act itself and any officer who is unsure about any aspect of RIPA should contact, at the earliest possible opportunity, the Senior Responsible Officer or the RIPA Co-ordinating Officer.

2. Policy Statement

2.1 The Council will comply with RIPA, appropriate codes of practice and any other relevant statutory provisions when it undertakes Covert Surveillance.

2.2 To this end, Covert Surveillance will only be undertaken if the procedures contained in this document have first been complied with.

3. Internal Governance

3.1 The Council has implemented a governance structure for the RIPA process to ensure that appropriate roles and responsibilities are in place and to enable effective oversight.

3.2 The Senior Responsible Officer will have overall responsibility for RIPA within the Council and will be responsible for ensuring the integrity of the process, compliance with RIPA, engagement with the IPCO at inspections and for overseeing the implementation of any recommendations made by an inspection. In addition s/he is required to ensure the standard of Authorising Officers. This means that s/he exercises ultimate overall oversight over the RIPA process.

3.3 The Senior Responsible Officer will not be responsible for authorising RIPA applications as this would affect his/her objectivity.

3.4 The Senior Responsible Officer will also be responsible for updating this Policy to ensure that it reflects any changes to legislation which the Council will need to adhere to. To ensure transparency, the Senior Responsible Officer will report to the Council's Strategy and Resources Committee annually so that the committee can ensure that RIPA use is consistent with the Policy and that the Policy remains sound.

3.5 The annual report will include details of the overall number and type of authorisations granted and the outcome of the case, where known. In addition, the annual report should also include the findings and recommendations of the most recent inspection carried out by a representative of the IPCO, where applicable (inspections may not take place annually). The Investigatory Power's Commissioner's Office has committed to try and visit local councils at least once in every three year period.

3.6 The role of Senior Responsible Officer will be undertaken by the Council's Monitoring Officer.

3.7 The officers named in Annex A shall be the only officers within the Council who can authorise applications under RIPA for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers. Authorising Officers may not carry out an authorisation (including a renewal or cancellation), until they have been certified by either the Senior Responsible Officer or the RIPA Co-ordinating Officer. Prior to obtaining authorisation, and throughout the term of any authorisation, Authorising Officers must follow the procedure at Annex D. Authorising Officers may not sub-delegate their powers in relation to RIPA to other officers.

3.8 The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

3.9 Authorising Officers must be properly trained in the relevant areas of authorisation and must be in a post of Director, Senior Manager or equivalent, or be undertaking a statutory appointment.

3.10 Authorising Officers will be removed from the list if they do not attend the required training programme(s) or if they fail to meet the required nationally recognised standards. The Annex will be kept up to date by the RIPA Co-ordinating Officer and amended as needs require. In addition, the RIPA Co-ordinating Officer has delegated authority to add, delete or substitute posts as required. If any of the Authorising Officers considers that a post should be added, deleted or substituted at Annex A, they shall refer such requests to the RIPA Co-ordinating Officer, for his/her consideration.

3.11 It is expected that the RIPA Co-ordinating Officer will undertake four functions:

- Maintenance of a central record of authorisations; collation of all original RIPA documentation;
- Day to day oversight of the RIPA process, particularly of the submitted documentation;
- Organising corporate training for RIPA; and
- Raising RIPA awareness within the Council.

3.12 All forms should be passed through the RIPA Co-ordinating Officer to ensure that there is a complete record of all authorisations. Content of the forms will be monitored to ensure they are correctly filled in and the RIPA coordinator will supply quarterly statistics to the Senior Responsible Officer.

4. What RIPA does and does not do

4.1 RIPA does:

- Require prior authorisation and judicial approval of directed surveillance;
- Prohibit the Council from carrying out intrusive surveillance;
- Require authorisation for the conduct and use of a CHIS; and
- Require safeguards for the conduct and use of a CHIS.

4.2 RIPA does not:

- Make unlawful conduct which is otherwise lawful;
- Prejudice or disapply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the Council's current powers to obtain information via the Land Registry as to the ownership of a property.

4.3 If the Authorising Officer or any officer is in any doubt, s/he should ask the Senior Responsible Officer before any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

5. What is meant by Surveillance?

5.1 "Surveillance" includes the following activities:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;
- Recording anything monitored, observed or listened to in the course of the surveillance; and
- Surveillance by or with the assistance of a surveillance device.

5.2 Surveillance may be either overt or covert. Surveillance is "covert" if it is carried on without the knowledge of the subject. Surveillance is "overt" if it is carried on with the knowledge of the subject. Planning enforcement staff may need to observe the activities of people suspected of breaching the planning laws, but such surveillance is done openly and is therefore overt.

5.3 Overt surveillance does not need RIPA authorisation. Covert Surveillance needs RIPA authorisation if it constitutes "directed surveillance" or "intrusive surveillance".

5.4 Surveillance is "directed" if it is (i) Covert, and (ii) is undertaken:-

- for the purposes of a specific investigation or operation;
- in such a manner as is likely to result in the obtaining of private information about a person or persons; and
- otherwise than by way of an immediate response to urgent circumstances, which would make it impracticable to obtain an authorisation for the surveillance.

5.5 An example of directed surveillance would be secretly keeping a person under observation in a public place or using a hidden camera to observe his or her movements or actions. If the person is aware that he or she is being observed or filmed the surveillance is overt and therefore is not "directed surveillance" for the purposes of RIPA. Regular viewing of a particular individual's social media account may also be regarded as "directed surveillance" for the purposes of RIPA, even if the social media account is unrestricted i.e. allows anyone to view its content.

5.6 Surveillance is "intrusive" if it is covert and

- is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

5.7 An example of "intrusive surveillance" would be the use of a bugging device in a private home or private vehicle. Local authorities are not authorised to carry out intrusive surveillance.

6. Covert Human Intelligence Sources

6.1 A CHIS[1] is a person who establishes or maintains a relationship with someone in order to covertly obtain information, to provide another person with access to information or to disclose information as a result of that relationship. An example of a CHIS would be an undercover police officer or an informant, or a child used to make a test purchase from a shop suspected of the underage sale of alcohol or tobacco. The use of a CHIS requires authorisation under RIPA.

6.2 An authorisation for the use of a CHIS may not be granted unless it is necessary:

a) in the interests of national security;

b) for the purpose of preventing or detecting crime or of preventing disorder;

c) in the interests of the economic well-being of the United Kingdom;

d) in the interests of public safety;

e) for the purpose of protecting public health;

f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

7. Use of directed surveillance and CHIS

7.1 The Council will not carry out "directed surveillance" or make use of a CHIS until it has been authorised by an Authorising Officer and an order approving the authorisation has been made by a Magistrates' Court.

7.2 Council officers can apply to an Authorising Officer for a RIPA authorisation for directed surveillance or the use of a CHIS if it is necessary to help them undertake their duties.

7.3 The role of the officer is to present to the Authorising Officer the following facts relating to the directed surveillance to be carried out:

- The crime being investigated;
- The reason why it is proposed to conduct the operation covertly;
- What covert tactics it is intended to use, and why; and
- The person who is to be the subject of the directed surveillance.

If the operation involves use of a CHIS, the officer must also present the following facts to the Authorising Officer:

[1] Further guidance can be found within the CHIS Code (publishing.service.gov.uk)

- The person who is to be used as the CHIS;

- What steps have been, or will be, taken to secure the welfare of the person used as the CHIS.

7.4 Officers seeking authorisation from an Authorising Officer for the use of directed surveillance or of a CHIS shall do so using the appropriate Home Office application form. The draft application form should be discussed with the Senior Responsible Officer, and the final wording checked with him/her before authorisation is sought.

7.5 The Authorising Officer will not authorise the use of directed surveillance unless the authorisation can be shown to be necessary for the purpose of preventing or detecting a criminal offence which either carries a maximum sentence of at least 6 months imprisonment or relates to the underage sale of alcohol or tobacco.

7.6 The Authorising Officer will not authorise the use of a CHIS unless the authorisation can be shown to be necessary for one of the purposes set out in section 6.2 of this Policy.

7.7 In addition, the Authorising Officer must believe that the use of directed surveillance or the use of a CHIS is necessary, reasonable and proportionate to what it seeks to achieve. In making this judgment, the Authorising Officer will consider whether the information can be obtained using other methods and whether efforts have been made to reduce the impact of the surveillance on people other than the person who is the subject of the operation.

7.8 Publicly available social media may be used to collect evidence, but officers must not use any false identity and must view a profile only on an ad hoc basis. Regular viewing of the same profile for the purposes of an investigation will need an authorisation for directed surveillance. Officers should seek to verify the information collected by other means.

8. Use of the Council's CCTV System

8.1 The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation.

8.2 However, the Council's CCTV systems shall not be used for directed surveillance in a covert and pre-planned manner as part of a specific investigation or operation unless a valid authorisation is in place. Regard should also be had to the provisions of the Protection of Freedoms Act 2012 relating to surveillance cameras and to any Code of Practice made thereunder.

9. Covert Surveillance of Social Networking Sites

9.1 The use of the internet and, in particular, social networking sites, can provide useful information for Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the Council for example Planning, Licensing or Environmental Health but can equally apply to non-enforcement teams, such as debt collection or Housing. The use of the internet and social networking sites may potentially fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the HRA.

9.2 When using social media for the gathering of evidence:

- officers must not “friend” individuals on social networks
- officers should not use their own private accounts to view the social networking accounts of other individuals
- officers viewing an individual’s profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation
- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual’s status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

9.3 If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual’s profile once in order to take an initial view as to whether there is any substance to the allegation or matter being investigated. The initial viewing must be reasonable, for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual’s profile or to print out several pages just in case they may reveal something useful.

9.4 In some cases, where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing. However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

9.5 Use of the internet is a useful tool and an authorisation for directed surveillance need only be sought where staff are ‘systematically collecting and recording information about a particular person or group ’. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by an Authorising Officer and then approved by a Magistrate. Further guidance as to the factors can be found at paragraph 3.16 of the Home Office Code of Practice “Covert Surveillance and Property Interference”

Guidance overview: Code of practice for covert surveillance and property interference - GOV.UK (www.gov.uk).

10. Obtaining Judicial Approval of Authorisations

10.1 Authorising Officers must, when making authorisations, be aware that each authorisation (or renewal of an authorisation) for the use of directed surveillance or for the use of a CHIS will be subject to the need for approval by the Magistrates’ Court. The Council will be required to make an application, without notice, to the Magistrates’ Court.

10.2 The Magistrates will give approval if and only if, they are satisfied that if at the date of the grant of authorisation or renewal of an existing authorisation there were reasonable grounds for believing that directed surveillance or use of a CHIS was necessary, reasonable and proportionate, that these grounds still remain and that the "relevant conditions" were satisfied in relation to the authorisation.

10.3 The relevant conditions referred to in the above paragraph are that:

- the relevant person was designated as an Authorising Officer;
- it was necessary reasonable and proportionate to believe that using directed surveillance or a CHIS was necessary, reasonable and that the relevant conditions have been complied with;
- the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and
- any other conditions provided for by an order made by the Secretary of State were satisfied.

10.4 Where the authorisation is for directed surveillance, the Magistrates' Court will also need to be satisfied that the directed surveillance is for the purpose of preventing or detecting a criminal offence which:

- is punishable by a maximum term of a least six months' imprisonment: or
- constitutes an offence under sections 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old); or
- constitutes an offence under section 92 of the Children and Families Act 2014 (sale of nicotine inhaling products to children under 18 years old) or proxy purchasing of tobacco, including nicotine inhaling products to children under 18 years old under section 91 of the Children and Families Act 2014.

10.5 Where the authorisation is for the use of a CHIS, the Magistrates' Court will also need to be satisfied that such use is for the one of the purposes set out in section 6.2 of this Policy.

10.6 If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

10.7 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained. To ensure compliance with this requirement, any Authorising Officer who proposes to approve an application for the use of directed surveillance or for the use of a CHIS must immediately inform the Senior Responsible Officer by telephone or e-mail of the details of the authorisation. The Senior Responsible Officer will then make the necessary arrangements for an application for an order to approve the authorisation to be made to the Magistrates' Court. The Authorising Officer and the investigating officer may be required to attend the Magistrates' Court to support the application.

11. Use of personal data obtained through the use of directed surveillance or of a CHIS

All personal data and sensitive personal data obtained using directed surveillance or a CHIS must be dealt with according to the provisions of the General Data Protection Regulation (**GDPR**) and of the DPA.

12. Impact Risk Assessment

12.1 When considering whether to carry out surveillance it is recommended that an 'impact risk assessment' (Annex C) is carried out and recorded to establish if the proposed course of action is a proportionate response to the problem it seeks to address. An impact risk assessment should be carried out on all activities including those that will not require RIPA authorisation. The form should be completed and submitted to an Authorising Officer.

12.2 The impact risk assessment involves:

- Identifying clearly the purpose(s) behind the monitoring arrangements and the benefits it is likely to deliver.

- Identifying any likely adverse impact of the monitoring arrangement.

- Considering alternatives to monitoring or different ways in which it might be carried out.

- Taking into account the obligations that arise from monitoring (especially on collateral intrusion

- Judging whether the monitoring is justified.

12.3 Adverse Impact- consideration should be given to:

- What intrusion, if any will there be into the private lives of workers and others, or interference with their private activities, emails, telephone calls or other correspondence.

- Whether those who do not have a business need to know will see information that is confidential, private or otherwise sensitive.

- In the case of surveillance on an employee, what impact, if any, will there be on the relationship of mutual trust and confidence that should exist between workers and their employer?

12.4 Alternatives – questions that should be asked:

- Are there other methods of obtaining the required evidence/information without carrying out covert surveillance, e.g. intelligence gathered from elsewhere.

- Has consideration been given to writing to the individual(s) informing them of the issue and advising that monitoring will be carried out over a specified period? (remember collateral intrusion could still apply to their colleagues or family etc.)

- Has consideration been given to carrying out overt surveillance as part of officers' normal duties?

- Can established or new methods of supervision, effective training and/or clear communication from managers, rather than electronic or other systemic monitoring, deliver acceptable results?

- Can monitoring be limited to those individuals and workers about whom complaints have been received, or about whom there are other grounds to suspect of wrongdoing?

- Can monitoring be automated? If so, will it be less intrusive, e.g. does it mean that private information will be 'seen' only by a machine rather than by other workers?

- Can spot-checks be undertaken instead of using continuous monitoring?

12.5 Obligations – means considering the following:

- Whether and how individuals or employees will be notified about the monitoring arrangements.

- How information about the individual or employee collected through monitoring will be kept securely and handled in accordance with RIPA and DPA requirements.

- The implications of the rights that individuals have to obtain a copy of information about them that has been collected through monitoring.

12.6 Justified – involves considering:

- The benefit of the method of monitoring/surveillance

- Any alternative method of monitoring/surveillance

- Weighing these benefits against any adverse impact

- Placing particular emphasis on the need to be fair to the individual worker or person

- Ensuring, particularly where monitoring electronic communications of employees is involved, that any intrusion is no more than is absolutely necessary.

13. Documentation and Central Register of Authorisations

13.1 Authorising Officers or Council officers may keep whatever records they see fit to administer and manage the RIPA application process. This will not replace the requirements under the Codes of Practice for the Council to hold a centrally held and retrievable record.

13.2 As cited in para 3.11 of this Policy, a central register of authorisations will be held by the RIPA Co-ordinating Officer and updated whenever an authorisation is refused, granted, renewed or cancelled. This central register should contain the following information:

- The type of authorisation
- The date the authorisation was given
- Name and grade of the Authorising Officer
- The unique reference number of the investigation
- The title of the investigation including a brief description and names of subjects

- Details of attendances at the Magistrates Court to include the date of attendance at court, the determining magistrate, the decision of the court and the time and date of that decision
- The dates of any reviews
- If the authorisation has been renewed, when it was renewed and who authorised the renewal including the name and grade of the Authorising Officer
- Whether the investigation is likely to result in obtaining confidential information as defined in the code
- Whether the authorisation was granted by an individual directly involved in the investigation
- The date the authorisation was cancelled
- The following documentation will also be held centrally:
    - A 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
    - A record of the period over which the surveillance has taken place
    - The frequency of reviews prescribed by the Authorising Officer
    - A record of the result of each review of the authorisation
    - A copy of any renewal of an authorisation together with any supporting documentation submitted when the renewal was requested
    - The date and time when any instruction to cease surveillance was given
    - The date and time when any other instruction was given by the Authorising Officer
    - A copy of the order approving or otherwise the grant or renewal of an authorisation from a JP/Magistrate

13.3 Authorising Officers shall notify the RIPA Co-ordinating Officer within 48 hours of the grant, renewal or cancellation of any authorisation and the name of the applicant officer to ensure the accuracy of the central register.

13.4 The records will be made available to the relevant Commissioner or an Inspector from IPCO, upon request. These records should be retained for at least five years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater.

14. Forms

The RIPA forms are available at www.gov.uk/government/collections/ripa-forms--2. If you do not have access to the internet, copies of these materials can be obtained from the RIPA Co-ordinating Officer.

15. Duration / Renewals

15.1 Renewals must take place prior to the authorisation expiring otherwise, the authorisation will automatically expire after three months in the case of direct surveillance and 12 months in the case of a CHIS. The duration of a juvenile CHIS is 4 months subject to at least monthly reviews to ensure that it is maintained for no longer than necessary.

15.2 Judicial Approval is required for a renewal. It is important to factor in sufficient time to obtain it well before the authorisation expires.

16. Reviews

16.1 The Authorising Officer should review all authorisations at intervals determined by him/her. This should be as often as necessary and practicable but in any event not less than monthly during the life of the authorisation for directed surveillance. The reviews should be recorded.

16.2 If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals.

16.3 The results of all such reviews shall be recorded on the central register of authorisations.

17. Cancellations

17.1 The Authorising Officer must cancel the authorisation if satisfied that the activity no longer meets the criteria upon which it was or could have been authorised or satisfactory arrangements for the source's case no longer exist. Where necessary, the safety and welfare of the CHIS should be considered after cancellation. At that point all directed surveillance must cease.

17.2 Records of cancellation are required to be kept. The cancellation form should detail what information has been obtained as a result of the surveillance activity. The forms should include the dates and times of any activity, the nature of the information obtained and the format, any associated log or reference numbers, details of where the product is to be held and the name of the officer responsible for its future management. Documentation of any instructions to cease surveillance should be retained and kept with the cancellation form.

18. Training

18.1 As stated in para 3.11 of this Policy, the RIPA Co-ordinating Officer will have responsibility for ensuring appropriate training is given to Authorising Officers, other senior managers and all likely applicants within the Council and for retaining a record of that training.

18.2 Any organised training may be by way of a briefing to Authorising Officers, an e-learning module or in-house training provided by external training consultants.

18.3 Refresher training for both applicants and Authorising Officers will be conducted at 18 monthly intervals.

18.4 Each Authorising Officer will receive a RIPA Authorising Officer Certificate following attendance at a training course.

19. Complaints

19.1 The Council will maintain the standards set out in this guidance and the current Codes of Practice. The Investigatory Powers Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by the legislation.

19.2 Contravention of the RIPA (and associated legislation) may be reported to the Investigatory Powers Commissioner at: Investigatory Powers Commissioner's Office PO Box 29105 London SW1V 1ZU Email: info@ipco.org.uk Telephone: 0207 389 8999

19.3 Contravention of the Data Protection Act 2018 and/or GDPR may also be reported to the Information Commissioner.

19.4 However before making such a reference, any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Monitoring Officer who will investigate the complaint. A complaint concerning a breach of this Policy should be made using the Council's own internal complaints procedure.

20. Where Can I Get More Advice?

20.1 This Policy cannot provide a definitive statement of the law, in all situations, nor a full description of all aspects of the Codes. If you have any doubt about whether a particular activity is lawful, you should always seek further advice from the RIPA Co-ordinating Officer contacting Katy Humphrey, tel. 01883 732700, email khumphrey@tandridge.gov.uk, in the first instance.

COMMUNICATIONS DATA

1. Acquisitions and disclosure of Communications Data

1.1 With effect from 5 January 2004, and in accordance with Chapter I of Part I of Regulation of Investigatory Powers Act ('the Act'), local authorities can authorise the acquisition and disclosure of 'communications data' provided that the acquisition of such data is necessary for the purpose of preventing or detecting crime or preventing disorder; and proportionate to what is sought to be achieved by acquiring such data. A link to the Home Office Code of Practice – Acquisitions and Disclosure of Communications data can be found here:

Codes of practice for the acquisition, disclosure and retention of communications data - GOV.UK (www.gov.uk)

1.2 The Protection of Freedoms Act 2012 made changes to the provisions under the Regulation of Investigatory Powers Act 2000 requiring the need for a local authority to seek judicial approval of the grant or renewal of an authorisation or of the giving or renewal of a notice.

1.3 NOTHING IN THIS CODE PERMITS THE INTERCEPTION OF THE CONTENT OF ANY COMMUNICATION.

1.4 The procedure is similar to that of authorisation for directed surveillance and CHIS but has extra provisions and processes. The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge. The Authorising Officer is called a 'Designated Person'

1.5 What is 'Communications Data'?

Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories:

- Traffic data - where a communication was made from, to whom and when
- Service data – use made of service e.g. Itemised telephone records
- Subscriber data – information held or obtained by operator on person they provide a service to.

Local authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

1.6 The application form should be completed via the National Anti- fraud Network website at www.nafn.gov.uk. The National Anti-fraud Network SPoC Service (acting as SPoC for the Council), will assess and quality control the application. If it meets the legal threshold for obtaining communications data, the SPoC will post it on the website for approval by the appropriate Designated Person. This procedure necessitates the applicant to be registered with the National Anti-fraud Network prior to making the application. For details on how to do this the applicant should visit www.nafn.gov.uk. If rejected, the SPoC will retain the application and inform the applicant in writing of the reason(s) for its rejection. Comprehensive guidance on the application process is also available via the National Anti-fraud Network website at www.nafn.gov.uk.

1.7 Authorisations can only authorise conduct to which Chapter II of Part I of the Act applies. In order to comply with the code, a Designated Person can only authorise the obtaining and disclosure of communications data if:

- it is necessary for any of the purposes set out in Section 22(2) of the Act. (NB the Council can only authorise for the purpose set out in Section 22 (2) (b) which is the purpose of preventing or detecting crime or preventing disorder);
- it is proportionate to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act).

1.8 Consideration must also be given to the possibility of collateral intrusion.

1.9 There are standard forms for authorisations and notice which are available using the link provided here:

RIPA forms - GOV.UK (www.gov.uk)

NAFN Home - National Anti Fraud Network

1.10 The Council is not permitted to apply or approve orally.

1.11 Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

1.12 An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

1.13 The code requires that all authorisations and notices should be cancelled by the Designated Person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant postal or telecommunications operator should be informed of the cancellation of a notice.

1.14 Under sections 23A and 23B of RIPA judicial approval from a magistrate must also be granted for all local authority requests for communications data.

1.15 Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner. Applications must also be retained to allow any Tribunal to carry out its functions.

1.16 A record must be kept of:-

- the dates on which the authorisation or notice is started or cancelled
- any errors that have occurred in the granting of authorisations or giving of notices

1.17 A report and explanation of any errors must also be sent to the Commissioner as soon as practicable.

1.18 Communications data and all copies, extracts and summaries thereof, must be handled and stored securely and the requirements of the Data Protection Act 2018 must be observed.

1.19 The RIPA Co-Ordinating Officer will maintain a centrally retrievable register.

1.20 The Investigatory Powers Commissioner shall provide independent oversight of the use of the powers contained in Part I and the code requires any person who uses the powers conferred by Chapter II to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions. The Act also establishes an Independent Tribunal to investigate and decide any case within its jurisdiction.

Annex A

ROLE	POST	POST HOLDER
RIPA Co-ordinating Officer	**Legal Specialist**	**Katy Humphrey**
Senior Responsible Officer	**Head of Legal**	**Lidia Harrison**
Authorising Officer	**Chief Executive**	**David Ford**
Authorising Officer	**Chief Planning Officer**	**Cliff Thurlow**
Authorising Officer	**Head of Localities**	**Simon Mander**

Annex B

RIPA AUTHORISING OFFICER CERTIFICATE

No:

I HEREBY CERTIFY that the officer whose personal details are given below is an Authorising Officer for the purposes of authorising covert surveillance and the use and/or conduct of Covert Human Intelligence Sources (**CHIS**) under the provisions of the Regulation of Investigatory Powers Act 2000.

It is further certified that this officer has received training to perform such authorisation procedures.

Certificate issued to: [Full name of officer]
Job title:
Location:
Certificate date:

(signed) .....

(PLEASE NOTE: This certificate and the authorisation granted by it is personal to the officer named in it cannot be transferred. Any change in personal details must be notified in writing to the **RIPA Co-ordinating Officer** immediately. This certificate can be revoked at any time by **Senior Responsible Officer** by written revocation issued to the officer concerned. It is the named officer's personal responsibility to ensure full compliance with RIPA authorisation procedures and to ensure that s/he is fully trained in such procedures and that such training is kept up to date).

ANNEX C

Impact Risk Assessment Form

Date and Time:

Name and Title:

Details of the operation / investigation

Details of the offence(s) / Breach(s)

Proposed actions

Purpose of the proposed actions and benefits it is likely to deliver

Identify any likely adverse impact of these actions

Are there any alternatives i.e. different ways in which the desired outcome could be achieved?

Are there any obligations that arise from the proposed actions?

How are these actions justified?

Does RIPA need to be considered?

Signature

Name of Officer

Date and Time

ANNEX D

RIPA Procedural Flowchart

The Investigating Officer (the **"Applicant") must:**

- Read the Council's RIPA Policy, Guidance Note for Officers and be aware of any other guidance issued by the SRO or RCO.
- Determine that directed surveillance and/or a CHIS is required.
- Assess whether authorisation will be in accordance with the law.
- Assess whether authorisation is necessary under RIPA and whether it could be done overtly.

If a less intrusive option is available and practicable, use that option

If authorisation is **necessary and proportionate**, prepare and submit the appropriate form and send to the RCO or other Authorising Officer.

The Authorising Officer must:

- Consider in detail whether all options have been duly considered, including the RIPA Policy and any other guidance issued by the SRO or RCO.
- Consider whether surveillance is considered by him/her to be necessary and proportionate.
- Authorise only if an overt or less intrusive option is not practicable.
- Set an appropriate review date (for periods not longer than monthly) and conduct the review.

THE APPLICANT IN CO-ORDINATION WITH THE RCO MUST OBTAIN APPROVAL FROM A MAGISTRATE

The Applicant must: review regularly and submit a review form to the Authorising Officer on date set.

The Applicant must: if the operation is no longer necessary or proportionate, complete the Cancellation Form and submit to the Authorising Officer.

The Authorising Officer must:
if surveillance is still necessary and proportionate:

- Review authorisation.
- Set an appropriate further review date.

Authorising Officer must:
Cancel authorisation when it is no longer necessary or proportionate to need.

ESSENTIAL:

Send all original RIPA documentation including Authorisation Forms, Reviews, Renewals and Cancellations to the RCO **within one week of the relevant event.**