Officer Guidance on RIPA

This Guidance supplements the Council's RIPA Policy and should be read in conjunction with it. Both documents are available on the Hub.

Definitions:

"**Authorising Officers**"	means senior officers of the Council who have received training in the application of RIPA. Only Authorising Officers have the power to authorise the use of a covert human intelligence source. Authorising Officers are listed at Annex A of the Council's RIPA Policy.
"**Codes of Practice**"	means Home Office Covert Human Intelligence Sources Revised Code of Practice (August 2018) and Home Office Covert Surveillance and Property Interference (August 2018) or any codes of practice issued in replacement of these codes.
"**Covert Surveillance**"	Surveillance will be covert if it is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.
"**Directed Surveillance**"	means surveillance is surveillance which: - is covert; - is not intrusive surveillance; - is undertaken for the purpose of a specific investigation or operation; - is undertaken in such a manner that it is likely that private information about an individual is obtained (whether or not that person is specifically targeted for the purposes of the investigation or operation); and - is not carried out by way of an immediate response to events, which would make seeking authorisation under the Act reasonably impracticable

"**Overt Surveillance**" Surveillance will be overt if the act of surveillance is not

calculated to be hidden from view, even if the motives of the person undertaking the surveillance remain concealed.

- "**RIPA Co-ordinating Officer**" or "**RCO**"

means the person responsible for the day-to-day oversight of applications, the maintenance of the central register and reporting to the Senior Responsible Officer of any failings, training needs or improvements to the system.

"**Senior Responsible Officer**" or "**SRO**"

means the Head of Legal and Monitoring Officer for Tandridge District Council.

"**Surveillance**" includes the following:

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications; or
- Recording anything mentioned above in the course of authorised surveillance; or
- Surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Background

1. The Regulation of Investigatory Powers Act 2000 (**RIPA**) is an Act of Parliament which regulates the powers of public bodies, including local authorities, to carry out surveillance and investigation which can be relied on in court proceedings. It was originally introduced to take account of technological changes such as the growth of the Internet.

2. The purpose of this guidance, which should be read in conjunction with the Council's RIPA Policy, is to explain the scope of RIPA, the circumstances where it applies, the procedures to be followed and provide guidance on the use of covert surveillance, including use of social networking websites and Covert Human Intelligence Sources ("**CHIS**").

3. The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and the Legal Department has copies to which staff can refer. The relevant Codes of Practice and associated guidance that relate to authorised Council surveillance activities are:

a. Home Office Code of Practice – Covert Surveillance;
b. Home Office Code of Practice – Covert Human Intelligence Sources;
c. Home Office Code of Practice – Acquision and Disclosure of Communications Data
d. Guidance from the Office of Surveillance Commissioners;
e. Protection of Freedoms Act 2012 - changes to provisions under the Regulation of Investigatory Powers Act 2000: Home Office Guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice; and
f. Guidance on Investigatory Powers Act 2016.

Review

4. The Council's RIPA Policy and this document are important for the effective and efficient operation of the Council's actions in relation to surveillance. This document and the Policy will therefore be kept under yearly review by the Senior Responsible Officer and the outcomes of this review will be presented to the Executive Management Team.

5. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Senior Responsible Officer at the earliest opportunity.

How has the Council implemented RIPA?

6. The SRO has overall responsibility for RIPA within the Council and is responsible for ensuring the integrity of the process, compliance with RIPA, engagement with the Investigatory Powers Commissioner's Office (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 s/he exercises overall oversight over the RIPA process. The SRO will not be responsible for authorising RIPA applications as this would affect his/her objectivity. A list of individuals who may authorise a RIPA application for onward consideration by a magistrate, can be found at Annex A of the Council's RIPA Policy.

7. The RCO is responsible for (i) collating all RIPA documentation and maintaining a central record of authorisations, (ii) day-to-day oversight of the RIPA process, particularly of the submitted documentation, (iii) arranging RIPA training for staff, and (iv) raising RIPA awareness within the Council, as further detailed in the RIPA Policy

8. All forms should be sent to the RCO to ensure that there is a complete record of all authorisations. Contents of the forms will be monitored to ensure that they are correctly filled in and the RCO will supply quarterly statistics to the SRO.

9. Any officer who is unsure about any aspect of RIPA should contact the SRO or the RCO for clarification.

10. The relevant Code recommends that elected Members of a local authority should review the authority's use of RIPA and set the policy at least once a year. Members should also consider internal reports on the use of RIPA on a regular basis to ensure it is being used consistently with the authority's policy and that the policy remains fit for purpose. This role is performed by the Council's Strategy and Resources Committee, which receives an annual assurance report about the use of RIPA powers and any recommended policy changes about the use (or not) of RIPA powers.

What does surveillance mean?

11. RIPA says “surveillance” means monitoring, observing and listening to persons, including their movements, communications, conversations and any other activities. It also includes the recording of anything being monitored in the course of surveillance, and the use of any listening device or photographic equipment. Note that regular viewing of an individual’s social media profile in the context of an investigation also constitutes surveillance under RIPA. Surveillance should be distinguished from the use of a CHIS (defined above), which is covered by the Act separately. RIPA defines two types of surveillance in relation to councils. These are directed surveillance and intrusive surveillance.

DIRECTED SURVEILLANCE

Surveillance becomes “directed surveillance” when:

- **It is covert, but not intrusive**: directed surveillance takes place within a public/quasi-public place, or where the tools used for surveillance are remote from the physical location. For example, a hotel lobby is deemed a public place, but a hotel room is private and therefore outside the scope of directed surveillance.
- **It is for the purpose of a specific investigation,** rather than for a general purpose. Several Council sites have CCTV operating for a general purpose of crime prevention and this is not subject to RIPA. However, if the same camera was used by a police officer for a specific purpose, RIPA would apply.
- **It is used to obtain private information about a person**.
- **It is not an immediate response to events.**

Examples of surveillance which would not be “directed surveillance”:

- Council officers openly observing the activities of residents whilst patrolling the streets, as part of activities to combat anti-social behaviour. Note “openly” means there must not be any deliberate effort to make sure individuals are unaware that this is taking place.
- Generally, the use of CCTV cameras, where these are properly signed.
- Routine planning enforcement visits, e.g. to check up on the physical development of a site.

- Covert surveillance of premises (as opposed to individuals) by environmental health officers, as part of their routine duties to detect statutory nuisances.
- The covert surveillance of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises, and the recording device is calibrated accordingly.
- Covert surveillance for the purposes of an "ordinary function", for example surveillance of an employee as part of a disciplinary process, (as opposed to covert surveillance for the purposes of a "specific public function" undertaken by the Council).

Does directed surveillance require authorisation?

Directed surveillance will always require authorisation. RIPA states that directed surveillance may only be authorised if it is both **necessary** and **proportionate** to what is sought to be achieved by carrying it out. Authorisation is a two-stage process. First, provisional authorisation must be obtained from one of the Council's Authorising Officers. Secondly, judicial approval must be obtained before any directed surveillance can be commenced. Section 28(3) RIPA defines "**Necessity**" as falling within one of the following categories:

- *In the interests of national security.*
- *Preventing or detecting crime or of preventing disorder.*
- *In the interests of the economic well-being of the UK.*
- *In the interests of public safety.*
- *Protecting public health.*
- *Assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.*
- *For any purpose other than those mentioned above which is specified by an order made by the Secretary of State.*

When can authorisation properly be given?

For local authority investigations, provisional authorisation for surveillance is deemed "necessary" in the circumstances of the particular case if it is for the purpose of the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale of alcohol or tobacco to underage persons, and if that objective could not be achieved without the information sought.

Conduct is not deemed “proportionate” if the pursuance of the legitimate aim listed in section 28(3) RIPA (in italics, above) will not justify the interference, i.e. if the means used to achieve the aim are excessive. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe. The conduct must also be the least invasive.

Officers considering that the necessary thresholds of necessity and proportionality have been met, should contact one of the Authorising Officers (at Annex A of the Council’s RIPA Policy) in order to obtain provisional RIPA authorisation. If the Authorising Officer concurs that the necessary thresholds have been met, he/she may grant “provisional” authorisation to make use of any of the RIPA powers. This provisional authorisation must be approved by the Magistrates Court before the use of the RIPA power in the investigation commences. All applications to the Magistrates Court will need to be made through the legal department.

Process for obtaining authorisation

If in doubt as to whether authorisation will be required, officers should contact the RCO to discuss the case in question. If the RCO considers that authorisation is required, the investigating officer will be asked to complete the following RIPA Authorisation Form and submit this to the RCO:

Form for the use of directed surveillance:

https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

Form for the renewal of the use of directed surveillance:

https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance

Form for the cancellation of the use of directed surveillance:

https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form

The forms are self-explanatory, however, guidance on completing the forms can be found by contacting the RCO or the RIPA team by email: commsdata@homeoffice.x.gsi.gov.uk

The RCO will log the case and will process the application him/herself or pass the matter to one of the other Authorising Officers to process.

The RCO or other Authorising Officer may only grant a “provisional” authorisation or renewal to make use of any of the RIPA powers. All provisional authorisations and renewals must be approved by the Magistrates Court before the use of the RIPA power in the investigation commences. Certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can only be granted by the Chief Executive Officer, or, in his/her genuine absence, another statutory officer.

The RCO or other Authorising Officer must apply to the local Magistrates Court for judicial approval of an authorisation or a renewal of an authorisation. It is not necessary to give notice of the application to the person(s) subject to the application or their legal representatives. If the Magistrates Court refuses to approve the application, they may also make an order quashing the provisional authorisation.

The Authorising Officer will provide the magistrate with a copy of the original RIPA provisional authorisation or notice and the supporting documents setting out the case. This forms the basis of the application and should contain all the information that is relied upon. The Magistrate will consider the provisionally authorised application or renewal, and will need to satisfy him/herself that:

1. At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;
2. That the person who granted provisional authorisation was an appropriately designated person;
3. The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and
4. Any other conditions provided for by an order made by the Secretary of State were satisfied.

The applicant in liaison with legal services is responsible for tabling the application in writing for judicial approval in the Magistrates Court before the use of the RIPA powers commence. The order section of the application form will be completed by the magistrate and will be the official record of his/her decision. The Council will need to obtain judicial approval for all initial RIPA authorisations / applications and renewals and will need to retain a copy of the judicial application order form after it has been signed by the magistrate. There is no need for the magistrate to consider either cancellations or internal reviews. The duration of an authorisation in the case of directed surveillance is three months. Cancellation is a positive act for which diary dates must be set. Authorisations can be reviewed at any time and should be cancelled

as soon as they are considered to be no longer necessary or appropriate. Forms are available for the cancellation and renewal of surveillance, as required.

All RIPA forms can be found at: https://www.gov.uk/government/collections/ripa-forms--2

INTRUSIVE SURVEILLANCE

Surveillance is deemed to be intrusive if it takes place either in:

- **Residential premises** or any **private vehicle**
- If it involves the **presence of an individual** on the premises or is carried out by means of a **surveillance device**.

Those authorising need to give careful consideration as to whether technology might make otherwise directed surveillance intrusive. An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.

When can intrusive surveillance be used?
As the name suggests, intrusive surveillance has a greater impact on an individual than directed surveillance, and consequently there are greater restrictions on the circumstances in which it can be deployed and the persons who may authorise it. **RIPA prohibits local councils from carrying out intrusive surveillance.**

SOCIAL MEDIA CONSIDERATIONS

Social media can allow us to accumulate a sizeable amount of information about an individual's life. It can therefore be a very useful tool when investigating alleged offences. It is crucial that the provisions of RIPA are considered when using social media in investigations, as depending on the actions of the investigator, this may cross over into the realm of directed surveillance. If correct authorisation is not obtained, then the Council's actions would become unauthorised surveillance, and in doing so, breach an individual's right to privacy under Article 8 of the ECHR. Even, where the surveillance has not breached Article 8, if the provisions of RIPA have not been properly followed, then the evidence obtained may be rendered inadmissible.

The definition of “private information” under RIPA includes “any information relating to a person’s private or family life and should be taken generally to include any aspect of a person’s private or personal relationship with others, including family and professional or business relationships”.

Privacy Settings

By setting a private profile, a user restricts access to their content and respect should be shown to that person’s right to privacy under Article 8 of the Human Rights Act 1998. This does not, however, extend to instances where a third party takes information and shares it on their own profile. For example, Person A has a private profile but a friend of theirs, Person B, takes something from Person A’s page and shares it on their public page. This cannot be used from Person A’s page, but could from Person B’s page.

Ad hoc viewing vs persistent viewing

Provided officers are careful only to gather information that is relevant to proving the offence they are investigating, then it is possible to view a public profile without requiring authorisation under RIPA. Once-off visits or infrequent visits to an individual’s Social Media profile spread over time cannot be considered “directed surveillance” for the purposes of RIPA. However, if the viewing becomes repeated, planned or directed, then Legal Services should be consulted in advance to obtain the relevant authorisation. It is important to note that even if an individual’s social media profile is unrestricted/in the public domain, this does not allow for repeated viewing of the site unless the correct authorisation has been obtained.

Each viewing of a company or individual’s social media profile for the purpose of an investigation must be recorded on the case log.

Unlike the GDPR, which is concerned with “personal information”, the provisions of RIPA apply to both businesses and individuals.

Officers must not use their own personal accounts when accessing social media sites for investigation purposes. Only Council accounts should be used. Interaction and dialogue of any kind should be avoided.

Evidence that is of a readable form, i.e. text, status updates or photographs should be copied directly from the site or captured via screenshot, onto a hard drive and subsequently printed to a hardcopy. The hardcopy of evidence should then be exhibited to a prepared witness statement in the normal way.

If evidence is audio or video then efforts should be made to download that content onto a hard drive or CD/DVD. Those CDs/DVDs should then be annexed to a suitably prepared witness statement in the normal way.

Screenshots – should display the time and date in order to provide when the evidence was captured. Without this information the effectiveness of the evidence is potentially lost as it may not be admissible in court.

When capturing evidence from a Social Media profile steps should be taken to minimise the collateral damage of inadvertently capturing innocent third parties' information. This might be particularly prevalent on Social Media profiles promoting events.

Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should be retained in accordance with the Data Protection Act 2018, the Freedom of Information Act 2000 and any other legal requirements including the Council's Record Management, Retention and Disposal Policy and Schedule.

WHEN WILL AN INVESTIGATION USING SOCIAL MEDIA REQUIRE AUTHORISATION?

Officers must keep in mind whether they will require a RIPA authorisation prior to accessing an individual's social media profile. Any viewing which is (i) more than "one-off" viewing, and (ii) is in connection with an investigation / trying to ascertain information about an individual, will require a RIPA authorisation. The RIPA form should be submitted to the RCO as soon as possible to start the process of obtaining authorisation.

THE USE OF A CHIS

A CHIS is a covert human intelligence source. A person is a source 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 paragraph (b) or (c);

(b) they covertly use such a relationship to obtain information or to 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.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source. This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

The Protection of Freedoms Act 2012 amended RIPA to make CHIS authorisations by local authorities subject to judicial approval. These changes mean that local authorities need to obtain an order approving the grant or renewal of a CHIS authorisation from a magistrate before it can take effect. If the magistrate is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the CHIS as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of CHIS.

WHO CAN PROVIDE CHIS AUTHORISATIONS?

The Council can authorise the use or conduct of a CHIS. Most CHIS authorisations will be for both use and conduct because authorities will usually task the CHIS to take covert action, and because the CHIS will be expected to take action, such as responding to the particular tasking. Care must be taken to ensure that the CHIS is clear on what is/is not authorised at any given time, and that all the CHIS's activities are properly risk assessed.

The relevant Code explains that, “the use or conduct of a CHIS can be a particularly intrusive and high-risk covert technique, requiring dedicated and sufficient resources, oversight and management”. Whether or not the use or conduct of a CHIS relates to private information, the covert manipulation of a relationship to gain information of any kind will engage the Article 8 rights, and therefore authorisation must be sought.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 as amended permits a “Director, Head of Service, Service Manager or equivalent” to grant authorisations. This will also include anyone in a more senior position. A list of Authorising Officers can be found at Annex A of the Council’s RIPA policy.

The Home Office prescribed forms must be used (links to these can be found on page 12, below). The Authorising Officer must believe that an authorisation for the use or conduct of a CHIS is “necessary” in the circumstances of the particular case on one of the grounds specified in section 29(3) of RIPA, which are as follows:

(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.

If deemed necessary, the Authorising Officer must also believe that it is “proportionate” to what is sought to be achieved by carrying it out. This involves, amongst other considerations, balancing the seriousness of the intrusion into the private or family life of the subject of the operation (or person who may be affected) against the need for the activity in investigative and operational terms. The following matters should also be considered in relation to “proportionality”:

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

- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others; and
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives of obtaining the necessary result; and
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

The relevant Code says that any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, Court.

The Council must appoint a “handler” who will have day-to-day responsibility for dealing with the CHIS on behalf of the Council, directing the day-to-day activities of the CHIS, recording the information supplied by the CHIS, and monitoring the CHIS’s security and welfare. Further, the Council must also appoint a “controller” who will be responsible for the management and supervision of the “handler” and for general oversight of the use of the CHIS.

Note also that an authorisation cannot take effect until such time as a magistrate has made an order approving the authorisation. The magistrate can only give approval if satisfied that there were, and still are reasonable grounds for the authorisation, and also that certain relevant conditions were satisfied. The Legal Team will deal with the application to the magistrate, and will notify you once such an order has been made. Legal will retain copies of the judicial application/order forms after they have been signed by the magistrate, and these will be kept in the Central Record together with the original authorisation.

PROCESS FOR OBTAINING CHIS AUTHORISATIONS

The process for obtaining authorisation for the use of a CHIS is similar to the process for obtaining authorisation for the use of directed surveillance. If the officer is satisfied that the twin requirements of necessity and proportionality (explained above) been met in the

circumstances, he/she must complete the relevant form (below) and submit this to the RCO for review by one of the Authorising Officers.

Form for applying for the use of a covert human intelligence source:

https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis

If the investigating officer has any issues with completing the form, he/she should consult the RCO or email the RIPA team: commsdata@homeoffice.x.gsi.gov.uk

As with the directed surveillance procedure, this authorisation (if given) is only provisional, and no action can be taken in relation to using/instructing the CHIS until approval has been obtained from the Magistrates' Court.

A written authorisation for a CHIS will, unless reviewed, cease to have effect at the end of 12 months, beginning with the day it took effect, except in the case of juvenile CHIS when it lasts for four months.