8.5.8. Where the purpose of a Communications Data application is to identify a journalistic source, these must first be authorized by an Authorising Individual (OCDA AO or DSO) but must also be approved by an IPCO Judicial Commissioner (JC). The Applicant and SPOC should pay special consideration to these applications and inform their Senior Responsible Officer. The IPA does not alter the existing processes for Communications Data applications that may feature sensitive professions including medical doctors, lawyers, journalists, parliamentarians, or ministers of religion. If the Communications Data could contain information relating to any of these professions, this must be noted in the application.

8.6. Urgency

8.6.1. Urgent authorisations are no longer available in relation to directed surveillance or covert human intelligence sources.

8.7. Standard Forms

8.7.1. All authorisations must be in writing.

8.7.2. The standard form for obtaining authorisation and judicial approval is provided at Appendix 2 . All authorisations shall be sought using the standard forms as amended from time to time.

9. Activities by other public authorities

9.1. The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

10. Joint Investigations

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

10.2. When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

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

b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms

should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency being involved in the RIPA activity of the external agency.

10.3. In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

11. Duration, Renewals and Cancellation of Authorisations

11.1. Duration

11.1.1. Authorisations must be reviewed in the time stated and cancelled once no longer needed. Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source (4 months for juvenile CHIS authorisations)

b) three months from the date of judicial approval for directed surveillance.

c) one month from the date of approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

11.1.2. However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

11.2. Reviews

11.2.1. The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations.

11.2.2. Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

11.2.3. The standard form to be used to record a Review can be found at Appendix 3 to this policy.

11.3. Renewals

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

11.3.2. Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired.

11.3.3. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

11.3.4. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

11.3.5. A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and
- the information obtained from the conduct or use of the source and
- for the purposes of making an Order, the Magistrates have considered the results of that review.

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

11.3.7. The standard form to be used to record the approval of a Renewal can be found at Appendix 4 to this policy

11.4. Cancellations

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

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

11.4.3. The standard form to be used to record the Cancellation of an authorisation can be found at Appendix 5 to this policy.

12. Records

12.1. The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the Assistant Director, Legal & Governance.

12.2. In relation to communications data, the designated SpoC will retain the forms and the Assistant Director, Legal & Governance, will have access to such forms as and when required.

12.3. Central Record of all Authorisations

12.3.1. The Assistant Director, Legal & Governance, shall hold and monitor a centrally retrievable record of all judicially approved authorisations. The Authorising Officer must notify and forward a copy of any notice or authorisation granted, renewed, or cancelled and any judicial approval received or refused within 1 week of the event to the Assistant Director, Legal & Governance to ensure that the records are regularly updated.

12.3.2. The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These records will be retained for a period of 5 years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

12.3.3. The Assistant Director, Legal & Governance, will monitor the submission of judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any draft document, as necessary. The records submitted to the Assistant Director, Legal & Governance, shall contain the following information:

a) the type of authorisation or notice

b) the date the authorisation or notice was given;

c) name and rank/grade of the authorising officer;

d) the date judicial approval was received or refused;

e) the unique reference number (URN) of the investigation or operation;

f) the title of the investigation or operation, including a brief description and names of subjects, if known;

g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;

h) whether the investigation or operation is likely to result in obtaining confidential information;

i) review dates

j) the date the authorisation or notice was cancelled.

12.4. Records maintained in the department.

12.4.1. The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any

b) supplementary documentation and notification of the approval given by the Authorising Officer;

c) a record of the period over which the surveillance has taken place;

d) the frequency of reviews prescribed by the Authorising Officer; a record of the result of each review of the authorisation or notice;

e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;

f) the date and time when any instruction was given by the Authorising Officer.

g) the unique reference number for the authorisation (URN)

12.4.2. Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

12.5. Other Record of Covert Human Intelligence Sources

12.5.1. Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant an authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

12.5.2. The records shall contain the following information:

a) the identity of the source;

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

c) any relevant investigating authority other than the Council;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

respect of the source's activities for the benefit of that or any other relevant investigating authority.

13. . Retention and Destruction

13.1. Material obtained from properly authorised surveillance, or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data.

13.2. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

13.3. Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

14. Consequences of ignoring RIPA

14.1. RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be lawful for all purposes.

14.2. Where there is interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

14.3. Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation.

14.4. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

15. Scrutiny of Investigating Bodies

15.1. The Investigatory Powers Commissioner's Office independently scrutinises the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioner will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at www.ipco.org.uk

15.2. There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from IPCO.

15.3. The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM THE ASSISTANT DIRECTOR, LEGAL & GOVERNANCE OR THE LEGAL TEAM

MEDWAY COUNCIL

List of Officers to issue authorisations under RIPA

Role	Directorate	Job Title	Person	Authorising Officer Training completed
Authorising Officer		Chief Executive	Richard Hicks	27/06/2023
Authorising Officer	BSD	AD Legal & Governance	Bhupinder Gill	27/06/2023
Authorising Officer	BSD	Head of Legal Services	Vicky Nutley	27/06/2023
Authorising Officer	BSD	Head of Internal Audit & Counter Fraud Shared Service	James Larkin	27/06/2023
Authorising Officer	RCE	Head of Regulatory Services	Ian Gilmore	27/06/2023