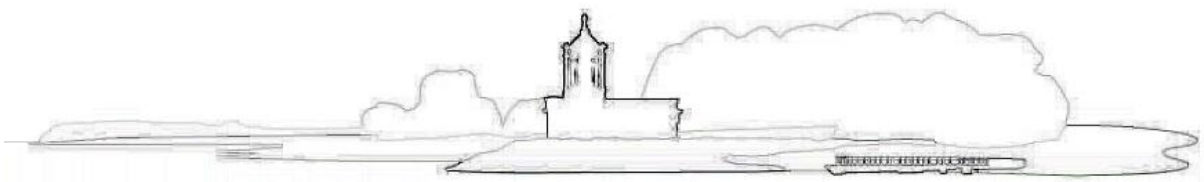
Rutland County Council

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

FOR THE USE OF COVERT SURVEILLANCE, COVERT HUMAN INTELLIGENCE SOURCES (CHIS) and THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Version & Policy Number	Version ~~2~~ 3
Guardian	Deputy Director Corporate Governance
Date Produced	December 2018
Next Review Date	November 2021

Approved by Cabinet	~~February 2019~~ PENDING APPROVAL



Contents

BACKGROUND

Rutland County Council ("the Council") only carries out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. It recognises its obligation to comply with RIPA when such an investigation is for the purpose of preventing or detecting crime or preventing disorder, and has produced this guidance document to assist officers

Applications for authority

An officer of at least the level of Director will act as Authorising Officer and consider all applications for authorisation in accordance with RIPA. Any incomplete or inadequate application forms will be returned to the applicant for amendment. The Authorising Officer shall in particular ensure that: -

a) there is a satisfactory reason for carrying out the surveillance
b) any directed surveillance passes the "serious crime" threshold
c) the covert nature of the investigation is necessary
d) proper consideration has been given to collateral intrusion
e) the proposed length and extent of the surveillance is proportionate to the information being sought.
f) Chief Executive's authorisation is sought where confidential Legal / medical / clerical / parliamentary / journalistic / spiritual welfare issues are involved
g) The authorisations are reviewed and cancelled.
h) Records of all authorisations are sent to Information Governance for entry on a Central Register.

Once authorisation has been obtained from the Authorising Officer, the Authorising Officer will attend the Magistrates' Court in order to obtain Judicial approval for the authorisation.

Training

Each Authorising Officer shall be responsible for ensuring that relevant members of staff are aware of the Act's requirements.

Refresher training shall be offered once a year via a Learning Pool E-Learning module (provided by Human Resources) to relevant Officers of the Council and also give advice and training on request.

Central register and records

The Information Governance Team shall retain the Central Register of all authorisations issued by the Council. The Information Governance Team will also monitor the content of the application forms and authorisations to ensure that they comply with the Act.

Senior Responsible Officer ("SRO")

The Senior Responsible Officer, a role required by the ~~Office of the Surveillance Commissioners (the "OSC")~~ Investigatory Powers Commissioner's Office (IPCO) and the Chief Surveillance Commissioner to the Investigatory Powers Commissioner's Office with oversight of the Council's use of RIPA powers is the ~~Deputy Director Corporate Governance~~ Monitoring Officer.

RIPA Co-ordinating Officer

The RIPA Co-ordinating Officer role, with the responsibility for the day-to-day RIPA management and administrative processes observed in obtaining an authorisation and advice thereon is performed by the Data Protection Officer.

1.0 RIPA - PART II DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1.1 PURPOSE

The purpose of this guidance is to explain:

a) the scope of RIPA – Part II;
b) the circumstances where it applies, and
c) the authorisation procedures to be followed.

1.2 INTRODUCTION

This Act, which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and approved by the judiciary before they are carried out.

In November 2016, the Investigatory Powers Bill received Royal Assent and is known as the Investigatory Powers Act 2016. The investigatory powers, which are relevant to a local authority, are directed covert surveillance in respect of specific operations, involving criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco, and the use of covert human intelligence sources ("CHIS"). The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use.

The policy should be read in conjunction with the Home Office Codes of Practice on covert surveillance and covert human intelligence sources; acquisition and disclosure of communications data, and any guidance issued by the Investigatory Powers Commissioner's Office (IPCO) ~~(formerly the Office of Surveillance~~

~~Commissioners – OSC).~~ Codes of Practices in relation to the use of these powers and these are attached at Appendix B & E.

Consideration must be given, prior to authorisation as to whether or not the acquisition of private information or the covert manipulation of a relationship is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be gleaned in other ways.

2.0 SCRUTINY AND TRIBUNAL

2.1 External Security and Tribunal

As of 1st November 2012 the Council has to obtain an order from a Justice of the Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity carried out. The Council can only appeal a decision of the Justice of the Peace on a point of law by Judicial review.

~~The Office of Surveillance Commissioners (OSC)~~ The Chief Surveillance Commissioner to the Investigatory Powers Commissioner's Office (IPCO) was set up to monitor compliance with RIPA. The ~~OSC~~ Chief Surveillance Commissioner to the IPCO has "a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA", and the Chief Surveillance Commissioner to the IPCO will from time to time inspect the Council's records and procedures for this purpose.

In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. Applications will be heard on a judicial review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

The Tribunal can order:

a) Quashing or cancellation of any warrant or authorisation;
b) Destruction of any records or information obtained by using a warrant or Authorisation;
c) Destruction of records or information held by a public authority in relation to any person.

The Council has a duty to disclose to the tribunal all documents they require if any Council officer has:

a) Granted any authorisation under RIPA
b) Engaged in any conduct as a result of such authorisation

2.2 Internal Scrutiny

The Council will ensure that the SRO is responsible for;

a) The integrity of the process in place within the Council to authorise directed surveillance and CHIS;
b) Compliance with PART II of the 2000 Act and with the accompanying Codes of Practice;
c) Engagement with the Commissioners and inspectors when they conduct their inspections and
d) Where necessary overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

The Elected Members of the Council will review the Council's use of the 2000 Act and the Council's policy and guidance documents at least once a year. Members will also consider internal reports on a regular basis throughout the year indicating the nature of RIPA activity undertaken or inactivity, to ensure that any use is consistent with the Council's policy and that the policy is fit for purpose. The Members will not however be involved in making decisions on specific authorisations.

2.3 Unauthorised Activities

If any Officer is concerned that surveillance/CHIS activity is taking place and there is no authorisation under RIPA in place, he/she should have contacted The Information Governance Team to seek advice.

If any activity is deemed to be unauthorised, it will be reported to the ~~OSC~~ Chief Surveillance Commissioner to the IPCO.

3.0 BENEFITS OF RIPA AUTHORISATIONS

The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, RIPA provides a statutory framework under which covert surveillance or CHIS can be authorised and conducted compatibly with Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

Material obtained through properly authorised covert activity is admissible evidence in criminal proceedings.

4.0 DEFINITIONS

4.1 **Covert** is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place.

4.2 **Covert Human Intelligence Source (CHIS)** is defined as a person who establishes or maintains a personal or other relationship with a person for the covert process of obtaining/providing access to/disclosing, information obtained through that relationship or as a consequence of the relationship.

4.3 **Directed surveillance** is defined as covert but not intrusive surveillance and undertaken:

a) for a specific investigation or operations;
b) in such a way that is likely to result in the obtaining of private information about any person;
c) other than by way of an immediate response.

4.4 **Private information** includes any information relating to a person's private or family life. Private information should be taken generally to include information on any aspect of a person's private or personal relationship with others including family and professional or business relationships.

4.5 **Intrusive** surveillance is covert surveillance that 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 using a surveillance device. Rutland County Council cannot authorise such surveillance.

4.6 **Authorising Officer** in the case of the Council, is the Chief Executive and Directors. If the operation concerns more than one Department in the Council, it can only be authorised by the Chief Executive.

5.0 WHEN DOES RIPA APPLY

Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary for the purpose of preventing or detecting crime or of preventing disorder.

The Council can only authorise Directed Surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or be an offence under:

a) Section146 of the Licensing Act 2003 (sale of alcohol to children)
b) Section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
c) Section 147A of the Licensing Act 2003 (persistently selling alcohol to children)
d) Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc. to persons under eighteen)

5.1 CCTV

The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV covertly and in a pre-planned manner as part of a specific investigation or operation to target a specific individual or group of individuals. Equally a request, say by the police,

to track particular individuals via CCTV recordings may require authorisation (from the police).

5.2 Online Covert Activity

The use of the internet and social media sites may be required to gather information prior to and during an operation/investigation. Officers should exercise caution when utilising such sites during an investigation and be alert to situations where authorisations under RIPA may be required. If officers have any concerns over the use of social media during an investigation they should contact their Line Manager. As a general rule of thumb however, reviewing open source sites such as Facebook pages where no privacy settings are in place does not require an authorisation under RIPA unless review is carried out with some regularity, often to build a profile, when directed surveillance authorisation may be required. If the officer then, for the purposes of gleaning intelligence breaches privacy controls and becomes for example a "friend" within a subjects Facebook account, utilising a pseudo account to conceal his/her identity as a Council official, this is a covert operation which, by its nature, is intended to obtain private information and should be authorised as a minimum as directed surveillance. Further, if the officer engages in any form of relationship with the account operator then s/he is likely to become a CHIS requiring authorisation and management by a Controller and Handler with a record being kept and a risk assessment created.

The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in 2018, provides the following guidance in relation to online covert activity:

'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

- *The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the*

Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

Page 11 of 24 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt, and a directed surveillance authorisation will not normally be available.

As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information. Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information.

Simple reconnaissance of such sites (i.e., preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.'

6.0 COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

6.1 The RIPA definition (section 26) is anyone who;

a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b) or c);
b) covertly uses such a relationship to obtain information or provide access to any information to another person; or

c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Any reference to the conduct of a CHIS includes the conduct of a source which falls within a) to c) or is incidental to it.

References to the use of a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

6.2 Section 26(9) of RIPA goes onto define

a) 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 that purpose; and
b) a relationship is used covertly, and information obtained as mentioned in above and is disclosed covertly, if, and only if it is used or as the case may be, disclosed in a manner that Is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

With any authorised use of a CHIS, the Council must ensure that arrangements are in place for the proper oversight and management of the CHIS, this includes appointing individual officers as handlers and controllers in relation to the CHIS. There is a risk that an informant who is providing information to the Council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised in the 2000 Act, not whether or not the CHIS is asked to do so by the Council. When an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship, it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on any information from such an informant.

6.3 Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. Paragraph 4.2 of the Home Office guidance 2018 on Covert Human Intelligence Source provides that:

On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility for him.

~~The duration of a juvenile CHIS is one month. The Regulation of Investigatory Powers (Juveniles) Order 2000 SI No. 2793 contains special provisions which must be adhered to in respect of juvenile sources.~~

In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 SI No. 2793 are satisfied.'

(https://www.legislation.gov.uk/uksi/2000/2793/contents/made)

Any authorisation of a juvenile CHIS must be granted by the Chief Executive.

6.4 Vulnerable Individuals

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age, or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Special consideration must be given to the use of a Vulnerable Individual as a CHIS. Emphasis must be placed on the operation of the provisions for the source's welfare. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances. Any authorisation of a vulnerable individual as a CHIS must be by the Chief Executive.

7.0 AUTHORISATIONS

7.1 Applications for directed surveillance

All application forms must be fully completed with the required details to enable the authorising officer to make an informed decision. Application forms are available on the Home Office website; officers should ensure they are using the most up to date forms for RIPA authorisations. The authorisation will only commence on the date Magistrates Court approval is obtained (see 7.6) and runs for three months from that date of that approval. No authorisation shall be granted unless the authorising officer is satisfied that the investigation is:

a) necessary for either the purpose of preventing or detecting crime or of preventing disorder;
b) Involves a criminal offence punishable whether summarily or on indictment by a maximum sentence of at least six months' imprisonment or related to the underage sale of alcohol or tobacco (see 5 for offences);
c) Proportionate - This has 3 elements, namely,
    - that the method of surveillance proposed is not excessive to the seriousness of the matter under investigation;
    - the method used must be the least invasive of the target's privacy;
    - the privacy of innocent members of the public must be respected and collateral intrusion minimised (see 7.1).
d) and that no other form of investigation would be appropriate;
e) The grant of authorisation should indicate that consideration has been given to the above points;
f) Advice should be sought from the Data Protection Officer on any issues of concern.

The Authorising Officer must take into account the risk of 'collateral intrusion' i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation. The application must include an assessment of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion.

Those carrying out the investigation must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as it becomes apparent. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

The Authorising Officer should also fully understand the capabilities and sensitivity levels of any equipment being used to carry out directed surveillance so as to properly assess the risk of collateral intrusion in surveillance techniques.

7.2 Special consideration in respect of confidential information

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved. Confidential information consists of matters subject to legal privilege, communication between a Member of Parliament and another person on constituency matters, confidential personal information, confidential constituent information or confidential journalistic material.

7.2.1 Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of Legal Services should be sought in respect of any issues in this area.

7.2.2 Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's spiritual welfare or matters of medical or journalistic confidentiality

7.2.3 Confidential journalistic

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence. It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 of the Freedom of Information Act 2000.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive, or, in his/her absence, a Chief Officer and should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

7.3 Authorisations

Authorisations must be in writing and have a “wet” signature.

7.4 Notifications to Inspector/Commissioner

The following situations must be brought to the inspector/commissioner’s attention at the next inspection:

a) Where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved;
b) Where a lawyer is the subject of an investigation or operation;
c) Where confidential personal information or confidential journalistic information has been acquired and retained.

7.5 Applications for CHIS

The process for CHIS applications is the same as for directed surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least 6 months in imprisonment does not apply. The authorisation must be in writing, must specify the activities and identity (by pseudonym only) of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

Again the Authorising Officer must be satisfied that the authorised use and conduct of the CHIS is proportionate to what is sought to be achieved by that conduct and the CHIS must be necessary for the prevention or detection of crime or the prevention of disorder.

All application forms must be fully completed with the required details to enable the Authorising Officer to make an informed decision. A risk assessment and record must be prepared for each CHIS.

7.6 Judicial Approval of authorisations (see guidance at Appendix C and D)

Once the Authorising Officer has authorised the Directed surveillance or CHIS, the Applicant and the Authorising Officer who gave the authorisation should

attend the Magistrates Court for the authorisation to be approved by a Justice of the Peace. In the event that the Applicant cannot be present, the Authorising Officer would need approval for rights of audience subject to Section 223 of the Local Government Act 1972. The hearing should ideally be on the same day as the Authorising Officer gives authorisation; the court should be contacted prior to attendance to ensure the matter can be heard.

The Authorising Officer will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition, the Authorising Officer will provide the Justice of the Peace with a partially completed judicial application/order form. These documents should be taken to the court by the Authorising Officer and not sent to the court by any other means prior to the hearing.

The hearing will be in private and the Authorising Officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate and whether that continues to be the case. They will also consider whether the authorisation was given by the appropriate designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

The Justice of the Peace can:

a) Approve the grant of the authorisation, which means the authorisation will then take effect for a period of three months;
b) Refuse to approve the grant of the authorisation, which means the authorisation will not take effect but the Council could look at the reasons for refusal, make any amendments and reapply for judicial approval;
c) Refuse to approve the grant of the authorisation and quash the original authorisation. The court cannot exercise its power to quash the authorisation unless the applicant has at least 2 business days from the date of the refusal in which to make representations.

No directed surveillance or CHIS action will be taken prior to approval by both the Authorising Officer and Magistrates Court.

7.7 Working in partnership with the Police

Authorisation can be granted in situations where the police rather than Rutland County Council require the surveillance to take action, as long as the behaviour complained of, meets all criteria to grant and in addition is also of

concern to the Council. Authorisation cannot be granted for surveillance requested by the police for a purely police issue.

The Police, as an emergency service may authorise RIPA without Magistrates approval, if an urgent situation arises and RIPA authorisation would be required urgently the Council should contact the Police.

8.0 UNIQUE OPERATION REFERENCE NUMBER

Each Application for Directed Surveillance and CHIS, must have a Unique Operation Reference Number. This URN will begin with either ENV (if it is granted in the Environment and Planning Department) or FIN (if it is granted in the Finance Department), followed by a sequential number, followed by 2018 being the year in which the Authority was applied for e.g. ENV/01/2018

9.0 DURATION AND CANCELLATION

An authorisation for directed surveillance shall cease to have effect (if not renewed or cancelled) 3 months from the date the Justice of the Peace approves the grant.

If renewed the authorisation shall cease to have effect 3 months from the expiry date of the original authorisation.

An authorisation for CHIS shall cease to have effect (unless renewed or unless juvenile) 12 months from the date the Justice of the Peace approves the grant or renewal.

This does not mean that the authorisation should continue for the whole period so that it lapses at the end of this time. The authorisation must be cancelled as soon as that officer decides that the surveillance should be discontinued.

On cancellation the cancellation form should detail what product has been obtained as a result of the surveillance activity. The forms should include the dates and times of the activity, the nature of the product obtained and its 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 instruction to cease surveillance should be retained and kept with the cancellation form.

10.0 REVIEWS

The Authorising Officer should review all authorisations at intervals determined by him/herself. This should be as often as necessary and practicable. The reviews should be recorded.

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. It would be appropriate to call a review specifically for this purpose.

Particular attention should be paid to the possibility of obtaining confidential information and an assessment as to the information gleaned should take place at every review.

11.0 RENEWALS

Any Authorising Officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect. The renewal must then be approved by the Justice of the Peace in the same way the original authorisation was approved. The process outlined in paragraph 7.6 should be followed for renewals.

A CHIS authorisation must be thoroughly reviewed before it is renewed.

12.0 CENTRAL REGISTER OF AUTHORISATIONS

12.1 All authorities must maintain the following documents:

a) Copy of the application and a copy of the authorisation form and the approval order from the Magistrates together with any supplementary documentation;
b) A record of the period over which the surveillance has taken place;
c) The frequency of reviews prescribed by the Authorising Officer;
d) A record of the result of each review of the authorisation;
e) A copy of any renewal of an authorisation and Order made by the Magistrates Court and supporting documentation submitted when the renewal was requested;
f) The date and time when any instruction to cease surveillance as given;
g) The date and time when any other instruction was given by the Authorising Officer.

To comply with 12. The Information Governance Team hold the central register of all authorisations issued by officers of Rutland county Council. The original authorisation, reviews, renewal and cancellation issued should be passed immediately to the Information Governance Team. A copy should be kept by the applicant Department and the Authorising Officer. Any original authorisations and renewals taken to the Magistrates Court should be retained by the Council, the court must only keep copies of the authorisations or renewals.

The Council must also maintain a centrally retrievable record of the following information:

a) type of authorisation;
b) date the authorisation was given;
c) details of attendance at the Magistrates' Court, the date of the attendance, the determining Justice of the Peace, the decision of the court and the time and date of the decision;
d) name and rank/grade of the Authorising Officer;
e) unique reference number of the investigation/operation;
f) title (including brief description and names of the subjects) of the investigation/operation;
g) whether urgency provisions were used, & if so why;
h) details of reviews;
i) dates of any renewals including the name and rank of the Authorising Officer;
j) whether the investigation/operation is likely to result in obtaining confidential information;
k) whether the authorisation was granted by an individual directly involved in the investigation;
l) date of cancellation.

These records will be retained for at least 3 years and will be available for inspection by the Office of Surveillance Commissioners.

13.0 RETENTION OF RECORDS

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance or CHIS. The Authorising Officers through their relevant Data Controller must ensure compliance with the appropriate data protection requirements under the UK General Data Protection Regulations (UK GDPR), Data Protection Act 2018 and any relevant codes of practice relating to the handling and storage of material. The Central Register of Authorisations will be kept securely in a locked cabinet in the Legal Services department.

From 2020, the Investigatory Powers Act 2016 and the Code of Practice (Appendix E) placed an obligation to ensure that any data that the council retains is stored properly and subject to a review, retention, and disposal process as part of the IPCO's Data Assurance Programme.

Reference to this can be found in the Investigatory Powers Commissioner's Annual Report 2020.

14.0 ~~COMPLIANTS~~ COMPLAINTS PROCEDURE

The Council will maintain the standards set out in this guidance and the Codes of Practice (See Appendix B & E). The Chief Surveillance Commissioner to the IPCO has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.

Contravention of RIPA may be reported to the Investigatory Powers Tribunal. Before making such a reference, a complaint concerning a breach of this guidance should be made using the Council's own internal complaints procedure. To request a complaints form, please contact the Data Protection Officer, Rutland County Council, Catmose, Oakham, Rutland, LE15 6HP or telephone 01572 758165 or dataprotection@rutland.gov.uk.

15.0 APPENDICES

Appendix A – Home Office RIPA Forms:
https://www.gov.uk/government/collections/ripa-forms--2

Appendix B - Covert Surveillance and Property Interference Code of Practice:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Appendix C – Home Office Guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

Appendix D – 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:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-wales.pdf

Appendix E – Covert Human Intelligence Sources – Code of Practice:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

A large print version of this document is available on request

Rutland County Council

Rutland County Council
Catmose, Oakham, Rutland LE15 6HP

01572 722 577
enquiries@rutland.gov.uk
www.rutland.gov.uk