Stoke-on-Trent City Council
REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) SURVEILLANCE

City of Stoke-on-Trent

ANNEX 4

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) SURVEILLANCE

June 2022

Contents

Part A – Introduction and RIPA General 4
1. Introduction 4
2. Purpose and Objectives 4
3. Overview Of The Law 4
5. Legislation and Codes Of Practice 7
Part B – Surveillance, Types and Criteria 8
6. Surveillance 8
7. Overt Surveillance 8
8. Covert Surveillance 8
9. Directed Surveillance (DS) Requirements 8
10. Test Purchases 9
Part C - Covert Human Intelligence Sources (CHIS) Requirements 10
11. Introduction 10
12. Restrictions on CHIS 11
13. Ongoing Contact and CHIS Details 11
14. Management of Sources 11
15. Vulnerable or juvenile sources 12
Part D – General Rules on Authorisations 13
16. Necessity, Proportionality and Collateral Intrusion 13
17. Confidential Information 14
18. Legal Privilege 14
Part E – Online Investigations 15
19. Internet and Social Media Investigations 15
20. Factors to consider before carrying out an online investigation 15
Part F – The Application and Authorisation Process 17
21. Preliminary 17
22. Relevant Forms 17
23. Application 17
24. Duration of Authorisations 18
25. Application to the Court 19
26. Decision of the Court 20
27. Post Court Procedure 20
28. Reviews of Authorisation 21
29. Renewals 21
30. Cancellations 22

31. Urgent Cases 22
Part G – Safeguarding the material and Central Record 23
32. Safeguarding and the use of surveillance material 23
33. Authorised Purpose 23
34. Handling and Retention of Material 23
35. Use of Material as Evidence 24
36. Dissemination of Information 24
37. Storage 25
38. Copying 25
39. Destruction 25
40. Central Records 26
Part H – Errors, Complaints and Contact Details 27
41. Errors 27
42. Complaints 27
43. Contact Details For This Policy 28
Appendix 1: Glossary 29
Appendix 2: Officer Roles And Responsibilities 34
Appendix 3: List Of Authorising Officers 36
Appendix 4: Applicants 37
Appendix 5: RIPA Procedures (Quick Guide) 39
Appendix 7: RIPA DS Flow Chart [Summary Only] 43
Appendix 8: List Of Forms On Intranet Site Under Part II Of RIPA 44

Part A – Introduction and RIPA General

1. Introduction

This document sets out the policy in relation to Stoke-on-Trent City Council's (the Council's) use of the Regulation of Investigatory Powers Act 2000 (RIPA) for the purpose of law enforcement and covers the use of Directed Surveillance and Covert Human Intelligence Sources.

It does not cover the acquisition and disclosure of communications data as this is governed under Annex 3 of the Corporate Surveillance Policy, titled "Acquisition and Disclosure of Communications".

Please note: This policy uses various expressions (capitalised), acronyms, legislation, statutory instruments, and guidance documents. To assist, a glossary is provided in Appendix 1.

2. Purpose and Objectives

RIPA allows the Council to undertake covert[1] surveillance, provided that it is in accordance with RIPA procedure, limitations and criteria set out in the formal documentation that must be used (**RIPA Forms**). Applications for Authorisation must be in writing; oral applications are not allowed.

Officers and agents working for the Council intending to launch or be involved in any surveillance must follow this RIPA policy. It is of the utmost importance that all such officers independently and actively consider relevance, criteria and the laws that apply to every need and request for surveillance including its implementation.

Only officers designated by this policy[2] have the roles and responsibilities under RIPA for this Council. A description of the individual roles and responsibilities are in Appendix 2 (Officer Roles and responsibilities) to this **policy**, which refers to the following:

1. RIPA Monitoring Officer – the Assistant Director - Governance and Registration who is also the designated Senior Responsible Officer who may delegate to a **RIPA Coordinator**

2. Authorising Officers

3. Applicants

If having read this document you are unclear about any aspect of the process, please seek advice from the Council's RIPA Co-ordinator on 01782 238871 or email legal.services@stoke.gov.uk.

3. Overview Of The Law

---

[1] "surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place" S.26(9)(a) Regulation of Investigatory Powers Act 2000

[2] See Appendix 3 (Authorising Officers) and Appendix 4 (Applicants) to this Policy.

Covert surveillance can constitute an interference with Article 8 of the European Convention on Human Rights, which provides that every individual has "a right to respect for his private and family life, his home and his correspondence". The Human Rights Act 1998 (HRA) provides that it is unlawful to interfere with those rights unless it is in accordance with the law, proportionate and necessary.

Under RIPA, the Council can conduct the following covert techniques:

- Directed Surveillance;
- Covert human intelligence source (CHIS)
- Acquisition and disclosure of data relating to communications[3]

The Home Office have published the following **mandatory**[4] Codes of Practice in respect of the surveillance activities that the Council can conduct:

- Covert surveillance and property interference code of practice
- Covert human intelligence sources code of practice
- Interception of communications and accessing communications data[5]

Whilst undertaking such activities the Council must ensure that the provisions of RIPA are observed including updates by way of additional Statutory Instruments.

The Council is only permitted to carry out Directed Surveillance for the purposes of preventing or detecting crime which is punishable by a maximum term of at least six months' imprisonment or if it is related to the underage sale of alcohol and tobacco or nicotine inhaling products[6].

The lawful criteria for CHIS authorisation is prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of six months' imprisonment.

The Investigatory Powers Commissioner's Office (IPCO) is the independent body which oversees the use of investigatory powers under RIPA and conducts inspections of local authorities to ensure they are compliant with RIPA.

An Investigatory Powers Tribunal will examine complaints from members of the public about the use of these powers.

[3] See Annex 3 of the Corporate Surveillance Policy

[4] RIPA: Part IV - Paragraph 71 (1)

[5] See Annex 3 of the Corporate Surveillance Policy

[6] Licensing Act 2003, sections 146,147 and 147A and Children and Young Persons Act 1933, section 7

4. Surveillance outside of RIPA

Surveillance activity that is neither directed nor intrusive is not regulated by RIPA.

This surveillance activity includes:

- surveillance that is not covert
- covert surveillance due to an immediate response to events
- covert surveillance due to general observation
- covert surveillance not related to the statutory grounds specified in RIPA
- overt use of CCTV and ANPR systems[7]
- covert surveillance authorised as part of an equipment interference warrant under the Investigatory Powers Act 2016
- other specific situations, e.g. voluntary interviewing by a member of a public authority, recordings of noise nuisance in certain circumstances[8].

Although such surveillance does not meet the criteria for RIPA, the Council must still comply with its obligations under the HRA and other applicable laws.

Therefore, non-RIPA surveillance must be:

- Necessary,
- Proportionate; and
- Take account of any safeguards and actual intrusion and ensuring that the decision making and other operations involved are recorded, whilst ensuring compliance generally.

In order to ensure a clear distinction between RIPA and non-RIPA Surveillance, the IPCO have recommended that the words 'directed surveillance' are not used on a non-RIPA application. A separate central record will also be kept clearly distinguishing between RIPA and non-RIPA authorisations. For example, an internal disciplinary investigation, which doesn't meet the criteria for directed surveillance.

[7] where overt CCTV, ANPR or other overt surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, a directed surveillance authorisation should be considered.

[8] ""Specific Situations where Authorisation is Not Available" 3.40 Covert Surveillance and Property Interference; Revised Code of Practice

5. Legislation and Codes Of Practice

In all cases, where RIPA will be applied, officers are required to consult RIPA and the relevant Codes of Practice, which include the following:

- **Regulation of Investigatory Powers Act 2000**

  http://www.legislation.gov.uk/ukpga/2000/23/contents

- **Regulation of Investigatory Powers Statutory Instruments**

  https://www.legislation.gov.uk/uksi/investigatory%20powers

- **Code of Practice for Covert Surveillance (Directed Surveillance):**

  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

- **Code of Practice for Covert Human Intelligence Sources (CHIS):**

  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

  At the time of updating this policy, there is a Draft Revised Code of Practice for Covert Human Intelligence Sources published in January 2021 which is expected to replace the 2018 guidance in due course. Therefore, please ensure you are using the correct guidance document.

- **Home Office Guidance to Local Authorities**

  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

In cases of doubt, please consult the RIPA Coordinator to interpret the legislative powers and duties.

Part B – Surveillance, Types and Criteria

6. Surveillance

Surveillance is:

- 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 surveillance, with or without the assistance of a device.

7. Overt Surveillance

Overt surveillance is where the subject of surveillance is aware that it is taking place, either by way of signage such as in the use of CCTV or because the person subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the Human Rights Act and be necessary and proportionate. Any personal data obtained will also be subject to the Data Protection Legislation.

8. Covert Surveillance

Covert Surveillance is defined as "surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place" and is covered by RIPA. Covert surveillance is categorised as either **intrusive** or **directed.**

There are three categories of covert surveillance regulated by RIPA: -

1. **Intrusive surveillance** (Local Authorities are not permitted to carry out intrusive surveillance).
2. **Directed Surveillance;**
3. **Covert Human Intelligence Sources** (CHIS).

9. Directed Surveillance (DS) Requirements

DS is Covert Surveillance carried out in a manner that is likely to obtain Private Information.

People have a reasonable expectation of privacy. If covert surveillance of activities is carried out (in public or otherwise) for future consideration or analysis, this is likely to involve procuring Private Information.

RIPA allows surveillance for the gathering of evidence under specific circumstances and in accordance with its rules on how it must be exercised. The Council is not permitted to undertake any activity which is likely to be Intrusive.

DS must be covert, but not intrusive, and:

- undertaken for the purposes of a specific investigation or operation and related to the prevention or detection of crime;
- is likely to obtain Private Information about a person (whether identified for the purposes of the investigation or not);

- is pre-planned and not by way of an immediate response to events or circumstances[9].

Restrictions

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 imposes restrictions on councils undertaking DS and can only be given full effect by Judicial Approval.

Authorising Officers cannot allow a DS unless it is for the purpose of preventing or detecting a criminal offence which is:

a. punishable by a maximum term of at least 6 months' imprisonment, or
b. constitutes an offence under:
    - Sections 146 (sale of alcohol to children), 147 (allowing the sale of alcohol to children) or 147A (persistently selling alcohol to children) of the Licensing Act 2003; or
    - Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under eighteen)[10].

Note that using DS for the purposes of tackling antisocial behaviour cannot be authorised, unless the behaviour constitutes a criminal offence carrying a maximum prison term of six months or more (option a).

10. Test Purchases

Test purchase activity does not in general require authorisation as a CHIS under RIPA as vendor-purchaser activity does not normally constitute a relationship as the contact is likely to be so limited. However, if a number of visits are undertaken at the same establishment to encourage familiarity, a relationship may be established and authorisation as a CHIS should be considered. If the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a Directed Surveillance authorisation if the surveillance meets the Directed Surveillance threshold which is covert surveillance which is likely to obtain private information and the offence carries 6 months or involves the sale of alcohol or tobacco to children. If it does not meet the threshold it is important that a full risk assessment takes place and the activity is justified and considers the Human Rights Act.

[9] RIPA 2000, Part II, s.26(2)

[10] The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012

When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent "fishing trips". Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed.

Part C - Covert Human Intelligence Sources (CHIS) Requirements

11. Introduction

RIPA provides for the use and management of a Covert Human Intelligence Source (**CHIS**).

Under RIPA[11], a person is a CHIS if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything in b. or c. (below)
(b) the relationship is covertly used to obtain information or to provide access to any information to another person; or
(c) information is disclosed covertly by the use of such a relationship or as a consequence of the existence of such a relationship.

A typical example of an activity using a source would be a Trading Standards Officer posing as a customer at a motor dealer's premises and engaging the salesperson in a conversation in order to uncover offences.

Any material/information obtained from a properly authorised source may be used as evidence in criminal proceedings. It is important to be aware of how the simple provision of information can lead to becoming a CHIS, if a source continues to provide information. This may be due to, say, further revelations due to that source's regular interaction, or relationship with an individual (e.g. neighbour). The circumstances may fulfil the requirements of CHIS and therefore, subject to the requirements set out in this section of this policy.

Legal advice should always be sought where consideration is given to the use of CHIS which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers. It doesn't matter whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information.

[11] Section 26(7) and (8) RIPA

12. Restrictions on CHIS

CHIS can only be used for the purpose of preventing or detecting a criminal offence. The serious crime criteria of the offence carrying a 6 month sentence does not apply to CHIS.

13. Ongoing Contact and CHIS Details

The investigating officer must record throughout the relationship the details of any type of contact with the CHIS on a Source Contact Sheet together with a Personal Data Sheet, which records details of the CHIS regarding identity, security and welfare. The forms are available and listed in Appendix 8 (List of forms available for use on Intranet Site under Part II of RIPA).

14. Management of Sources

RIPA places duties on the Council for the effective management of CHIS. These duties include:

Tasking

This is the assignment given to the source by their "handler", asking the source to obtain information, provide access to information or otherwise facilitate a flow of information. The source's designated contact will have day to day responsibility for:

- dealing with the source on behalf of the Council
- directing day to day activities of the source
- recording information supplied by the source in accordance with the Regulation of Investigatory Powers (Source Records) Regulations 2000; and
- monitoring the source's security and welfare

Authorisations may cover a range of activities under which the source may be tasked. If however, it is intended to task the source in a new or significantly greater way than originally authorised, the Authorising Officer should be informed and consideration given to completing a separate authorisation form.

Management Responsibility

Clear management arrangements must be in place for all sources. The source will have a designated person for day to day contact ("the Handler") normally the Investigating Officer or Team Leader. It will be the responsibility of each department to record any form of contact held with the source during the course of the authorised activity.

In addition, section 29(5)(b) of the Act requires the appointment of a controller, who will normally be responsible for the management and supervision of the handler and general oversight of the use of the CHIS. A controller must be appointed for each CHIS and the controller will be responsible for all of the responsibilities specified in section 29(5)(b) of the Act.

Security and Welfare

The Council must take account of the welfare of the source in authorising or tasking of a source. Before authorisation, the Authorising Officer should ensure that a Risk Assessment form has been completed to determine risk to the source of any tasking and the likely consequences should the role of the source become known. The relevant Risk Assessment form needs to be completed by the Investigating Officer.

Ongoing security and welfare and also post cancellation of the authorisation should be monitored.

The Investigating Officer is responsible for informing the Authorising Officer of any concerns which might affect:

- the validity of the risk assessment
- the conduct of the source, and
- safety and welfare of the source.

15. Vulnerable or juvenile sources

A vulnerable individual is a person who 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. Such individuals should only be authorised to act as a source in the most exceptional circumstances. In these cases, the City Director must be the Authorising Officer.

Special safeguards also apply to the use of juvenile sources under the age of 18 years. Juveniles should only be authorised to act as a source in the most exceptional circumstances. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. Authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. Authorisations for juvenile sources should only be granted by the City Director. The duration of such authorisations is four months.

Part D – General Rules on Authorisations

16. Necessity, Proportionality and Collateral Intrusion

Necessity

The Council is restricted to surveillance for Necessary purposes. When completing the application for Authorisation for covert surveillance it is, therefore, crucial to explain why surveillance is Necessary to achieve the objectives and that there were no other means of obtaining the same information in a less intrusive method.

Proportionality

The activity will not be Proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted are the least possible Intrusion on the subject and others;
- whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.[12]

Collateral Intrusion

Measures should be taken, wherever practicable, to avoid or minimise unnecessary Intrusion into the lives of those not directly connected with the investigation or operation.

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 same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

All applications must therefore include an assessment of the risk of collateral intrusion and detail the measures taken to limit this to enable the Authorising Officer fully to consider the proportionality of the proposed actions. This is detailed in a section within the authorisation form.

In order to give proper consideration to collateral intrusion, an Authorising Officer should be given full information regarding the potential scope of the anticipated

surveillance, including the likelihood that any equipment deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the Authorising Officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. It may also need retaining under CPIA. The Authorising Officer should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Legislation.

Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.

In the event that authorised surveillance unexpectedly and unintentionally interferes with the privacy of any individual other than the intended subject, the authorising officer should be informed by submitting a review form. Consideration should be given in any such case to the need for any separate or additional authorisation.

17. Confidential Information

In cases where it is likely that knowledge of Confidential Information will be acquired, authorisation must be obtained from the City Director. Authorisation is sought from the highest seniority within the Council due to the sensitive nature of Confidential Information and the need to offer such information an enhanced level of protection.

18. Legal Privilege

Any evidence or information that is subject to Legal Privilege cannot be used.

Communications and items are not subject to Legal Privilege when they are in the possession of a person who is not entitled to possession of them or if held or oral communications are made with the intention of furthering a criminal purpose.

Part E – Online Investigations

19. Internet and Social Media Investigations

Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

The internet is another method of carrying out surveillance and a computer is a surveillance device. Repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation may constitute Directed Surveillance. Activities of monitoring through, for example, a Facebook profile for a period of time and a record of the information is kept for later analysis or evidential purposes is likely to require a RIPA authorisation. Where covert contact is made with another person on the internet a CHIS authority may be required.

Where this is the case, the application process and the contents of this policy should be followed.

Where the activity falls within the criteria of surveillance or CHIS outside of RIPA, again this will require authorising on a non RIPA form which will be authorised internally.

20. Factors to consider before carrying out an online investigation

- Consider whether the evidence gathering is likely to result in obtaining private information about a person or group of people.
- Online investigations capable of interfering with a person's rights to private or family life should only be used where necessary and proportionate. You should consider proportionality and whether your actions achieve a balance between the public interest and rights of the individual. Please consider whether there are other ways to achieve your objectives.
- If the information is open source, i.e. in the public domain, it is unlikely to require a RIPA authorisation. However, if you are investigating a potential criminal offence and you carry out repeat viewing of this information in order to build up a picture, then it is likely that a RIPA authorisation for Directed Surveillance is required and this policy must be complied with. For example, you should not monitor a social media profile on a daily or weekly basis without considering a RIPA authorisation.
- If you are investigating a potential criminal offence, you will likely need to apply for a CHIS authorisation where you intend to engage with others online without disclosing your identity, e.g. by creating a false account and becoming a friend on Facebook. A Directed Surveillance authorisation should

also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

- You must only use a Council account. Do not use your own personal account to access social media sites for investigations. Please contact the Council's digital manager in the Communications Team and your line manager for approval before creating team or service accounts.
- You must only collect information to further the investigation that is relevant to proving the offence you are investigating.
- You should consider whether you are likely to identify or record information about third parties, such as friends or family of the subject of interest and therefore constitute Collateral Intrusion into the privacy of these individuals.
- You should fully record your actions, the options you considered and what factors influenced your decision.
- Retain information in accordance with Data Protection Legislation.
- Where the activity falls within the criteria of surveillance or CHIS outside of RIPA, this will require authorising internally by your line manager.
- If you need advice, please contact the Council's RIPA Co-ordinating Officer.

Part F – The Application and Authorisation Process

21. Preliminary

Direct Surveillance and the use of a CHIS can only be lawfully carried out if properly authorised.

Applications for DS/CHIS can only be made by an Applicant who is listed in Appendix 4 (List of Applicants) as nominated by each Department and trained to the standards required (a contemporaneous list of training is held centrally by the RIPA Coordinator).

An Applicant must consider each situation carefully for the purposes of surveillance. The Applicant needs to actively consider other means of gathering evidence and properly discount them prior to seeking Authorisation for a DS/CHIS. DS/CHIS cannot be used because it is easier or quicker.

Applicants must ensure that, if DS/CHIS is appropriate, the premises or place chosen for surveillance are suitable and safe for staff including Health and Safety, the existence of suitable emergency exits, toilet facilities, and rest areas or secure means of passage.

If professional witnesses are going to be used they must be contractually obliged to comply with RIPA and this policy indemnifying the Council against failure to do so.

If a feasibility study is proposed Authorisation will still be required if it involves observations and recordings relating to the actions of others without their knowledge.

22. Relevant Forms

The template forms for seeking authorisations, reviewing, renewing or cancelling a DS or CHIS are set out in Appendix 8 to this policy.

There is a very brief generic guide included in this policy in Appendix 5: (RIPA Procedures – Quick Guide) that provides a quick overview.

23. Application

Prior to completing an Authorisation Form, a Unique Reference Number (**URN**) must be obtained from the RIPA Coordinator.

The application form (see Appendix 8 List of Forms available for use on Intranet Site under Part II of RIPA) must be completed by an Applicant for submission to an Authorising Officer for approval.

It is the responsibility of the Applicant to ensure that the application form is completed and contains the following details:

- the precise details of the investigation, who will take part and any equipment to be used and the nature of the surveillance proposed
- why the authorisation is Necessary (the Council is restricted on its categories for surveillance – for the purposes of preventing or detecting crime and a description of the crime is included)
- why the authorisation is considered proportionate to what it seeks to achieve
- the level of authority required for the surveillance, i.e. the rank of the Authorising Officer

- details of Collateral Intrusion as a result of the surveillance and its justification
- details of Confidential Information that is likely to be obtained as a consequence of the authorisation (NOTE: Authorisation will be needed from the City Director) and, include details relating to potential Legal Privilege
- subsequent records of whether authority was given or refused, by whom and time and date.

A DS/CHIS requires initial authorisation from an Authorising Officer (listed in Appendix 3 – List of Authorising Officers). An Authorising Officer must also be trained to the standards required (a contemporaneous list of training is held centrally by the RIPA Coordinator).

An Authorising Officer cannot authorise an investigation in which they are directly involved.

The Applicant presents the completed form to an Authorising Officer who will assess whether the proposal for DS / CHIS is both Necessary and Proportionate before signing it.

The Authorising Officer's assessment involves balancing the importance and need to gather evidence against the level of potential intrusion on the target, and Collateral Intrusion. The latter should be minimised as much as possible.

The Authorising Officer should also assess and indicate whether the evidence could be obtained through less intrusive means recording whether all reasonable alternatives have been considered.

Authorising Officers must also note that:

a. There is **no** "one size fits all" catalogue or approach to any Authorisation/Review etc.
b. The Authorising Officer must:
    - not simply consider the type of tactic proposed/used and
    - use their discretion to allow or disallow authorisation etc. which can only be exercised by first considering the particular facts of the activity proposed.

Authorising Officers must record ***in their own words*** what they have considered and the reason for their decision directly on RIPA forms themselves.

24. Duration of Authorisations

Authorisations must be given for the maximum duration from the date approved by the Magistrates Court, but reviewed on a regular basis and formally cancelled when no longer needed.

They do not expire, they must be cancelled when the surveillance / CHIS is no longer proportionate or necessary.

Durations[13] are detailed below:

- Directed Surveillance - 3 months
- Renewal - 3 months
- Covert Human Intelligence Source - 12 months
- Renewal - 12 months
- Juvenile Sources - 4 months
- Renewal - 4 months

Officers should ensure that authorisations only last for as long as is considered necessary and proportionate.

25. Application to the Court

Following authorisation, the Applicant must apply to the local Magistrates Court for Judicial Approval[14].

Applying for Judicial Approval requires completion of the Court's application form, submission of the original authorisation with supporting documentation and contacting the Magistrates Court (or Court with a higher jurisdiction) to arrange a hearing.

It is important to ensure that ALL evidence is contained within the application in order to support the case including the Authorising Officer's own comments.

It is necessary for the Applicant (who has sufficient knowledge of the investigation and the requirements of RIPA) to attend the hearing as the Court may request clarification.

If required, the Authorising Officer can also attend the hearing as the applicant can't answer questions directed for the Authorising Officer. If not present all comments made by the court should be promptly reported to the Authorising Officer who will take action to incorporate or address them.

Oral presentations to the Court will NOT form part of the application. If legal support is required, please contact Legal Services.

---

[13] **Important Note:** expiry dates shall **always** be the day before the anniversary of grant or renewal etc. (e.g. Granted/reviewed on 25th and the relevant expiry will be the 24th of the relevant month/week).

[14] For guidance see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

For Judicial Approval, the Applicant (or Authorising Officer) must have authority to act on the Council's behalf under Section 223 of the Local Government Act 1972. If an Applicant requires such authority, a template letter is available, which must be signed by a Director with delegated authority to provide this under the Council's Constitution. This letter is evidence of authority if requested by the Court. Without such authority, the Court may not allow it to be relied upon in any prosecution proceedings.

The Court will consider the application for Judicial Approval and apply the same tests of Necessity and Proportionality.

26. Decision of the Court

The court has a number of options which are:

Approve or renew an authorisation. If approved by the court, the date of the approval becomes the commencement date for the duration of the three months and the officers are now allowed to undertake the activity.

Refuse to approve or renew an authorisation. The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the court to determine whether the authorisation has met the tests, and this is the reason for refusal, the officer should consider whether they can reapply. For example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

For, a technical error (as defined by the court), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve or renew and quash the authorisation. This applies where the court refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case, the officer will inform Legal who will consider whether to make any representations.

The court will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

The Council may only appeal a court decision on a point of law by judicial review. If such a concern arises, please consult Legal Services.

27. Post Court Procedure

It will necessary to work out the cancellation date from the date of the approval and ensure that the Applicant and Authorising Officer is aware.

Original copies of the completed Application Form (whether authorised or refused) together with a copy of the Judicial Approval, should be forwarded to the RIPA

Coordinator for inclusion in the Central Records. The Applicant should retain a copy for their own records.

Where dates are set within the process, e.g. review dates, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Code of Practice and reduce the risk of errors.

28. Reviews of Authorisation

Reviews should be under taken during the authorised period to assess the on-going need for DS/CHIS. The level of review will be determined by the Authorising Officer in the context of and according to the nature of the investigation, taking into account intrusion into private life, Collateral Intrusion and Confidential Information. A review should be as frequent as is considered necessary and practicable, but should be at least monthly.

The standard form for review must be completed by the Applicant and is referred to in Appendix 8 (List of forms available for use on Intranet Site under Part II of RIPA).

The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted for judicial approval.

The Applicant submits the review form to an Authorising Officer, who is personally required to write on the form:

- a confirmation to continue the DS/CHIS or not;
- a brief summary of the information obtained to date;
- a note on the issues of Necessity, Proportionality and risk of Collateral Intrusion;
- Confidential Information obtained.

Original copies of these forms when completed and authorised by the Authorising Officer must be forwarded to the RIPA Coordinator for inclusion within the Central Records.

29. Renewals

A renewal form is to be completed by the applicant when the original authorisation period is about to expire but the DS or CHIS is still required.

Renewals must be granted prior to the expiry of the current judicial approval for a further period of 3 months in the case of DS or 12 months' for a CHIS.

Applications for renewal of an authorisation are completed using the standard form listed in Appendix 8 (List of Forms available for use on Intranet Site under Part II RIPA).

The Applicant must complete the application for renewal and include the following information:-

- whether it is the first renewal, or details of every occasion on which the authorisation has been renewed previously
- any significant changes to the information supplied in the original application
- reasons why it is Necessary and Proportionate to continue the surveillance or use the source

- content and value to the investigation/operation of the information so far obtained / tasks given to the source during the period and the information obtained
- results of reviews of the investigation / source
- Consideration of Confidential Information, Legal Privilege and Collateral Intrusion

Authorisation of renewals is given by an Authorising Officer, after which, Judicial Approval must be obtained. Authorisations may be renewed more than once providing they continue to meet the criteria for authorisation and they are subject to Judicial Approval.

Once Judicial Approval is obtained the documents must be forwarded to the RIPA Coordinator for inclusion in central record.

If the Authorising Officer refuses to renew the application, the cancellation process should be completed.

30. Cancellations

If an authorised DS/CHIS is no longer needed or the criteria for authorisation no longer applies (including those that have expired) the authorisation must be cancelled without delay.

The Applicant must complete all sections of the cancellation form (see Appendix 8 (List of Forms available for use on Intranet Site under Part II RIPA) and seek authorisation to cancel from an Authorised Officer, preferably the one who granted it originally.

To cancel the Authorising Officer must be satisfied that the use of the surveillance no longer meets the criteria for authorisation and is no longer needed.

Every authorisation regarding the same investigation must be cancelled.

When cancelling a CHIS authorisation, an assessment of the welfare and safety of the source should also be assessed and any issues identified.

Notification of cancellations must be recorded on the form and forwarded to the RIPA Coordinator for retention in Central Records.

All departments must ensure that their departmental register is kept and which holds a copy of all of the forms submitted to the RIPA Coordinator. Copies of the relevant forms must be retained for a period of at least 5 years. It is the responsibility of each department to regularly review such a register and ensure that it is kept in a safe and secure place.

Do not wait until the expiry of the authorisation to cancel. Cancel it at the earliest opportunity when no longer necessary and proportionate.

31. Urgent Cases

On the rare occasions where out of hours access to a magistrate is required then it is for the Council to make local arrangements with the relevant HM Courts and Tribunals Service (HMCTS) staff. In these cases, the Council will need to provide two partially completed judicial application/order forms so that one can be retained by the magistrate/Judge. The Council will provide a copy of the signed application/order form to the court the next working day. Purely oral applications are not permitted.

Part G – Safeguarding the material and Central Record

32. Safeguarding and the use of surveillance material

The Council should ensure that its actions when handling information obtained by means of covert surveillance or CHIS activity comply with relevant legal frameworks and the Codes of Practice, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including Data Protection requirements, will ensure that the handling of private information obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards. The material will also be subject to the Criminal Procedures Investigations Act (CPIA).

33. Authorised Purpose

Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of the RIPA codes, something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA Act in relation to covert surveillance or CHIS activity;
- Is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- Is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

34. Handling and Retention of Material

All material associated and obtained with an application will be subject of the provisions of the Data Protection Legislation and CPIA Codes of Practice. All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained, together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

If an appeal against conviction is in progress when released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

If retention is beyond these periods it must be justified under Data Protection Legislation. Each relevant service within the Council may have its own provisions under their Data Retention Policy which will also need to be consulted to ensure that the data is retained lawfully and for as long as is necessary. For any data retained, there must be regular data reviews to ensure that retention of data is justified.

35. Use of Material as Evidence

Material obtained through Directed Surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1996 and the Human Rights Act 1998.

Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council will be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the Prosecuting Solicitor. They in turn will decide what is disclosed to the Defence Solicitors.

There is nothing in RIPA which prevents material obtained under Directed Surveillance authorisations from being used to further other investigations

36. Dissemination of Information

It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or shared outside with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

The obligations apply not just to the Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Officer In Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

A record will be maintained justifying any dissemination of material. If in doubt, seek advice.

37. Storage

Material obtained through covert surveillance and CHIS authorisations, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material. It will be necessary to ensure that both physical and IT security and an appropriate security clearance regime is in place to safeguard the material.

38. Copying

Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained.

39. Destruction

Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

40. Central Records

The Council's central record will be maintained by the Council's RIPA Co-ordinator.

The Applicant must ensure that all of the original DS and CHIS applications, reviews, renewals and cancellations are provided to the RIPA Coordinator. They should be forwarded as soon as possible after they have been granted (or refused) by the Authorising Officer and the Courts.

The RIPA Coordinator will hold the above documents together with any supporting documentation in a retrievable form. The central records will contain the following information regarding authorisations:

- The URN
- If refused by the Authorising Officer, a brief explanation of the reason why.
- If granted, the type of authorisation (i.e. DS or CHIS)
- Date of authorisation
- Name and rank/grade of the Authorising Officer Title of the investigation/operation including a brief description and names of subjects, if known
- Whether the urgency provisions were used and, if so, why
- 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 date of any reviews;
- If the authorisation was renewed, when it was renewed and who authorised it
- Whether the investigation/operation was/is likely to result in obtaining Confidential Information
- The date authorisation was cancelled.

In addition to the original authorisations there will be a need to provide a record of the duration of the surveillance, a copy of all renewals, reviews and subsequent cancellations. If any officer does not provide this documentation, the Senior Responsible Officer may remove such officer from the list in Appendix 3 (List of Authorising Officers) and/or Appendix 4 (List of Applicants) who shall no longer be authorised to authorise or pursue applications.

Records of authorisations will be retained by the RIPA Coordinator for a period of five years and will be made available to the IPCO on request.

Part H – Errors, Complaints and Contact Details

41. Errors

Errors can have significant consequences on an affected individual's rights. Proper application of RIPA, the Codes of Practice and this Policy should reduce the scope for making errors.

All staff involved in the RIPA process must report any issues to the RIPA Coordinator so it can be assessed whether it constitutes an error which needs reporting.

There are two types of errors within the Codes of Practice:

- Relevant error; and
- Serious errors

Relevant Error

A relevant error is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This includes compliance by public authorities with Part II of RIPA.

Examples of relevant errors occurring would include circumstances where:

- Surveillance or CHIS activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Codes of Practice.

All relevant errors must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and a full report within 10 working days. The report should include information on the cause of the error; the amount of surveillance conducted and material obtained or disclosed; any unintended collateral intrusion; any anaylsis or action taken; whether any material has been retained or destroyed and a summary of the steps taken to prevent recurrence.

Serious Errors

The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

42. Complaints

Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Senior Responsible Officer who will investigate the complaint.

A complaint can also be made to the Investigatory Powers Tribunal. They have jurisdiction to investigate and determine complaints against any public authority's use of RIPA powers, including those covered by this Policy.

Complaints should be addressed to:

The Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

43. Contact Details For This Policy

Please tell us if you need this document in large print, on audio tape, computer disc or in Braille.

Contact us on Tel. 01782 234567

Minicom 01782 232331

Please contact us if you have any difficulty reading this or require any further information

The RIPA Coordinating Officer

Legal Services

Stoke-on-Trent City Council,

Civic Centre,

Glebe Street,

Stoke on Trent,

ST4 1HH

Email: legal.services@stoke.gov.uk

Tel: 01782 238871

Appendix 1: Glossary

EXPRESSION	MEANING
ANPR	Automatic Number Plate Recognition
CCTV	Closed Circuit Television - in this context: a form of observation camera (or CAM) linked to a monitor or monitoring system;
CHIS	Covert Human Intelligence Sources;
Code of Practice	a document issued by a Central Government department detailing how an operation of a legally-based activity shall be conducted;
Collateral Intrusion	an intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation;
Confidential Information	Confidential Personal Information or Confidential Journalistic Information;
Confidential Journalistic Information	material acquired for the purposes of journalism and held subject to an undertaking to hold it in confidence;
Confidential Personal Information	information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it (an example of such information would be a patient's medical records held by a health professional);
CHIS or Covert Human Intelligence Source	establishing or maintaining a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that covertly:

EXPRESSION	MEANING
	▪ uses such a relationship to obtain information or to provide access to information to another person; or ▪ discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship ▪ Section 26(8)(a)-(c) RIPA;
Covert Surveillance	surveillance carried out in a manner calculated to ensure that persons subject to the surveillance are unaware it is taking place - Section 26(9)(a) RIPA 2000;
Council	the Council of the City of Stoke-on-Trent;
Data Protection Legislation	the UK General Data Protection Regulation, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended and the guidance and applicable codes of practice issued by the Information Commissioner

DS or Directed Surveillance	covert surveillance, but not intrusive, and undertaken: ▪ for a specific investigation or operation (for the prevention or detection of crime) ▪ in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation); and ▪ not as an immediate response to events, which would otherwise make seeking authorisation under the Act unreasonable (e.g. spotting something suspicious and continuing to observe it) ▪ Section 26 (2) RIPA;
HRA	the Human Rights Act 1998;
IPCO	Investigatory Powers Commissioner's Office
Intrusive/Intrusion	surveillance, if covert, and: ▪ carried out in relation to anything taking place on residential premises or in a private vehicle; and ▪ involves the presence of an individual on the premises or vehicle or is carried out by a surveillance device - Section 26(3) RIPA;

Intrusive Surveillance	A covert surveillance activity that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device - 2.11 Covert Surveillance and Property Interference; Revised Code of Practice), the Council is not permitted to carry out this type of surveillance;
Judicial Approval	agreement or authorisation by a court (given by a Magistrate or district or other rank of Judge;
Legal Privilege	communications between a professional legal adviser and the adviser's client or any person representing that client made in connection with the giving of legal advice to the client, also applies to those communications which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings (Police Act 1997);
Necessary/Necessity	for the purposes of preventing or detecting crime or preventing disorder (punishable by a maximum term of at least 6 months' imprisonment);
Policy	this document headed "REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) SURVEILLANCE"
Proportionate/ Proportionality/Proportional	involving balancing the intrusiveness of a surveillance activity on the target and others who might be affected by it (Collateral Intrusion), against the need for the activity;

Private Information	any information relating to a person's private or personal relationship with others including family, professional and business relationships - Section 26 (10) RIPA;
RIPA	the Regulation of Investigatory Powers Act 2000;
RIPA Forms	the forms or documents required for surveillance related actions under RIPA (listed below);
Social Media	electronic means of communication to subscribed individuals or generally available to or sent to the public or a section of it and generated by individuals or groups (such as Facebook, Twitter, YouTube, Reddit, Vines, Instagram, Second Life, blogs, content communities, and other niche communities, etc.);
Surveillance	an activity: ▪ monitoring, observing, listening to persons, their movements, conversations, other activities or communications ▪ recording anything monitored, observed or listened to in the course of surveillance ▪ Surveillance, by or with, assistance of a surveillance device - Section 48(2) RIPA;
URN	Unique Reference Number.

Appendix 2: Officer Roles And Responsibilities

Senior Responsible Officer

The Assistant Director – Governance & Registration (Monitoring Officer) is the Council's designated Senior Responsible Officer ('SRO')

The SRO is responsible for ensuring that the requirements of RIPA are complied with and are applied in a fair and consistent manner by various directorates within the Council.

The SRO is responsible for the following:

- The integrity of the process in place within the Council to authorise Directed Surveillance and the use of CHIS, managerial control and oversight of the quality of authorisations;
- Compliance with all relevant statutory provisions and associated guidance;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both of the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner Office (IPCO) and Inspectors who support the Commissioner when they conduct their inspections;
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner; and
- Ensuring that all Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

RIPA Coordinator

A solicitor in Legal Services is appointed to act on the SRO's behalf as the RIPA Coordinator.

The RIPA Coordinator:

- Maintains the Central Record of authorisations, renewals and cancellations.
- Keeps copies of the forms and the signed approval or refusal documentation from the magistrates for five years.
- Organises and maintains a RIPA training programme
- Maintains a record of RIPA training by Applicants and Authorised Officers
- Provide administrative support and guidance on the processes involved
- Raises awareness of RIPA within the Council
- The RIPA Coordinator is responsible for monitoring the progress of all of the authorisations made by the relevant departments and keeping an accurate account of such authorisations in the form of Central Records. It is the responsibility of each department to forward all original authorisation documentation to the RIPA Coordinator. Upon receipt, the RIPA Coordinator needs to ensure that the activity has been properly authorised, reviewed, renewed and cancelled at the appropriate time. Additionally, the RIPA Monitoring Officer is required to retain a record of all of the authorised surveillance activity carried out by the relevant department.

Authorising Officer

Appendix 3 lists the Authorising Officers whom can authorise covert surveillance.

The Act specifies that such a nominated person must be of an appropriate seniority. The Authorising Officer will therefore generally be a Director, Assistant Director or a Team Leader/Group Manager and shall be fully trained accordingly. Authorising Officers are not directorate specific and therefore any directorate may use any of the Authorising Officers listed.

The role of the Authorising Officers is to consider whether to authorise, review, or renew an authorisation. They must also officially cancel the RIPA covert activity.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation, the central record of authorisations should highlight this, and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

Authorisations must be given in writing by the Authorising Officer by completing the relevant section on the authorisation form. When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

Authorising Officers must explain why they believe the activity is both necessary and proportionate, having regard to the collateral intrusion. They must also consider any similar activity which may be taking place or sensitivities in the area.

They also need to explain exactly what they are authorising, against who, in what circumstances, where etc. It is important that this is made clear on the authorisation as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors.

If any equipment, such as covert cameras are to be used, the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

The Authorising Officer may be required to attend court to explain what has been authorised and why.

Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that Authorising Officers hold their own copy of this document.

Applicant

There is a list of Applicants at Appendix 4 who are the only officers that can complete applications for DS and CHIS. These persons have been specifically authorised by the Senior Responsible Officer as designated by their manager for this role and have

received training in respect of RIPA and completing applications correctly, taking in to account both necessity and proportionality as detailed in this policy. Any applications made by officers not listed as an Applicant will not be accepted due to non-compliance with this policy, as they would not have received the appropriate training and require authorisation from the Senior Responsible Officer to be added to the list of Applicants.

The role of the Applicant is more particularly described within each type of surveillance as set out in this policy however, it will be the task of the Applicant to complete any applications, reviews, renewals and cancellations and obtaining the requisite approval from an Authorising Officer.

The Applicant is likely to attend court to seek the approval of the magistrate and if approved and involved in the covert activity they must only carry out what is authorised and approved.

Appendix 3: List Of Authorising Officers

Job Title	**Directorate**
Strategic Manager Regulatory Services	Regulatory Services, Housing, Development and Growth
Strategic Manager Audit and Fraud	Corporate Fraud Team Strategy and Resources
Corporate Fraud Team Manager	Corporate Fraud Team Strategy and Resources

Appendix 4: Applicants

Job Title	Directorate & Team
Corporate Fraud Investigator X 3	Corporate Fraud Team Strategy and Resources
Senior Corporate Fraud Investigator	Corporate Fraud Team Strategy and Resources
Principal Trading Standards Officer	Public Protection Adult Social Care, Health Integration and Wellbeing
Health Protection Manager	Public Protection Adult Social Care, Health Integration and Wellbeing
Consumer Protection Manager	Public Protection Adult Social Care, Health Integration and Wellbeing
Lead Officer Investigations and Consumer Protection	Public Protection Adult Social Care, Health Integration and Wellbeing
Trading Standards Officer X 3	Public Protection Adult Social Care, Health Integration and Wellbeing
Environmental Crime Team Leader	Regulatory Services Housing, Development and Growth Directorate
Traffic and Statutory Compliance Officer	Regulatory Services Housing, Development and Growth Directorate
Principal Licensing Officer	Regulatory Services Housing, Development and Growth Directorate

Job Title	Directorate & Team
Planning Enforcement Officer X 2	Planning and Development Control Housing, Development and Growth Directorate

Appendix 5: RIPA Procedures (Quick Guide)[15]

RIPA allows the Council to carry out covert surveillance in a regulated manner for the prevention and detection of crime or preventing disorder.

The Council maintains the various forms required on Stoke Inside (Intranet). A detailed guidance on DS and CHIS are set out in this policy. A quick guide on the procedural steps needed is given in this section which provides officers with a summary to obtaining authorisation for covert surveillance. Officers must, in any event, be fully acquainted with the full policy on RIPA (including the relevant laws) and the associated Guidance Notes on each topic.

Preliminary Warnings:

1. Cameras must NOT be installed or any covert surveillance started without first obtaining the requisite Authorisation
2. Only a designated Applicant who has received the requisite training can make a RIPA application.
3. Only a designated Authorising Officer who has received the requisite training can grant Authorisations
4. All the forms referred to below are available on Stoke Inside
5. Expiry dates shall always be the day before the anniversary of grant or renewal etc. (Granted / reviewed on 25th, the relevant expiry will be the 24th of the relevant month).

Step 1: Application

The Applicant contacts the RIPA Coordinator for a Unique Reference Number that must be used for that DS or CHIS and on all its forms and generally throughout.

Step 2: Submission

The Applicant completes the appropriate Application Form (DS or CHIS) and submits it to the Authorising Officer.

Step 3: The 5Ws

The Authorising Officer considers the contents of the Application and must actively consider and apply the 5Ws prior to granting or refusing Authorisation by writing the answers to them in the Application Form:

1. ***why*** *is the surveillance necessary,*
2. ***whom*** *is the surveillance directed against,*
3. ***where*** *and 4.* ***when*** *will it take place,*
5. ***what*** *surveillance activity/equipment is sanctioned and how is it to be achieved?*

Step 4: Authorisation Granted/Refused

[15] See also Appendix 6 (Guidance Form of Authorisation For DS) and Appendix 7 (RIPA DS Flow Chart – Summary Only)

a. The Authorising Officer completes and signs the Application after endorsing upon it **how** the Application satisfies the 5Ws (avoiding a mere statement that it does) and returns it to the Applicant.
b. If the Authorising Officer does not grant or approve the Application, the Authorising Officer draws a line through the Application with the heading 'REFUSED' returning it to the Applicant.

IMPORTANT NOTE:

If, at any time (including post Step 5: Judicial Approval), the RIPA Monitoring Officer considers that the Applicant or Authorising Officer has not actively considered the 5Ws the RIPA Monitoring Officer shall ensure that the Applications is cancelled/withdrawn and ensure that all further actions or activities based upon it are ceased immediately.

Step 5: Judicial Approval

The Application must be submitted to the Court for Judicial Approval and a hearing arranged for this purpose. If the Court provides Judicial Approval, surveillance can commence and lasts for 3 months (DS) or 12 months (CHIS)[16].

Step 6: Retention of Copies

The Applicant, upon grant or refusal, shall retain a copy of the Application and forward the original to the RIPA Coordinator for retention in the Central Record.

Note: Ensure all documents and maps referred to in the Application are attached to copies of it on submission to the Central Record.

Step 7: Reviews

The Applicant shall monitor the Authorisation and activities under it submitting a Review at least every month[17].

The Applicant shall complete any Review Forms, which must be signed by an Authorising Officer, a copy retained and the original sent to the RIPA Coordinator.

Step 8: Renewals

If an Authorisation is due to expire and a Renewal is required[18]; the Applicant must complete a Renewal Form and seek authorisation from the Authorising Officer. If a Renewal is granted judicial approval, it is obtained as in Step 5: Judicial Approval (which lasts for a further 3 months[19]). If it is refused, the procedure is the same as Step 4: Authorisation Granted/Refused - (b).

---

[16] **Important Note:** expiry dates shall **always** be the day before the anniversary of grant or renewal etc. (e.g. Granted/reviewed on 25th and the relevant expiry will be the 24th of the relevant month/week).

[17] Ibid, on how anniversary dates are calculated.

[18] Ibid, on how anniversary dates are calculated.

[19] Ibid, on how anniversary dates are calculated.

The Applicant retains copy of a Renewal and forward original to the RIPA Coordinator (whether Renewal granted or refused).

Step 9: Cancellation

Once an Authorisation is no longer required or has expired; the Applicant completes a Cancellation Form, to be signed by an Authorising Officer, retain a copy and send the original to the RIPA Coordinator.

Appendix 6: Guidance Form Of Authorisation For DS

The document is an internal document for employees using RIPA.

Appendix 7: RIPA DS Flow Chart [Summary Only]

The document is an internal document for employees using RIPA.

Appendix 8: List Of Forms On Intranet Site Under Part II Of RIPA

The document is an internal document for employees using RIPA.

DIRECTED SURVEILLANCE FORMS (DS):

1. APPLICATION
2. REVIEW
3. RENEWAL
4. CANCELLATION

COVERT HUMAN INTELLIGENCE SOURCE FORMS (CHIS):

1. APPLICATION
2. REVIEW
3. RENEWAL
4. CANCELLATION