APPENDIX 1

Rushmoor Borough Council
Policy for
Owner:

RBC/Corporate/001

RUSHMOOR BOROUGH COUNCIL

Surveillance and Regulation of Investigatory Powers Act 2000 (RIPA)

Policy and Guidance

N.B. Staff should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

Status: Draft
Approved by:

Issue Date:

DRAFT

Contents

Section PART A - Introduction & RIPA General

1. Introduction
2. Scope of Policy
3. Background to RIPA and Lawful Criteria
4. Consequences of Not Following RIPA
5. Independent Oversight

Section PART B - Surveillance, Types and Criteria

6. Introduction
7. Surveillance Definition
8. Overt Surveillance
9. Covert Surveillance
10. Intrusive Surveillance Definition
11. Directed Surveillance Definition
12. Private Information
13. Confidential or Privileged Material
14. Lawful Grounds
15. Test Purchases
16. Urgent Cases
17. Surveillance for Preventing Disorder
18. CCTV
19. Automatic number Plate Recognition (ANPR)
20. Internet and Social Media Investigations
21. Surveillance Outside of RIPA
22. Joint Agency Surveillance
23. Use of Third-Party Surveillance
24. Surveillance Equipment
25. Communications Data

Section PART C - Covert Human Intelligence Sources (CHIS)

26. Introduction
27. Definition of CHIS
28. Vulnerable CHIS
29. Lawful Criteria
30. Conduct and Use of a Source
31. Handler and Controller
32. Undercover Officers
33. Tasking
34. Risk Assessments
35. Use of Equipment by a CHIS
36. CHIS Management
37. CHIS Record Keeping

37.1. Centrally Retrievable Record of Authorisations
37.4. Individual Source Records of Authorisation and Use of CHIS
37.9. Further Documentation

Section PART D - RIPA Roles and Responsibilities

38. Senior Responsible Officer (SRO)
39. RIPA Co-Ordinator
40. Managers Responsibility and Management of the Activity
41. Investigating Officer/Applicant
42. Authorising Officer
43. Necessity
44. Proportionality
45. Collateral Intrusion

Section PART E - The Application and Authorisation Process

46. Relevant Forms
47. Durations
48. Application/Authorisation
49 Arranging the court Hearing
50. Attending the Court Hearing
51. Decision of the J.P.
52. Post Court Procedure
53. Reviews
54. Renewals
55. Cancellation

Section Part F - Central Record & Safeguarding the material

56. Introduction
57 Central record
58. Safeguarding and the Use of Surveillance Material
59. Authorised Purpose
60. Handling and Retention of Material
61 Use of Material as Evidence
62. Dissemination of Information
63. Storage
64. Copying
65. Destruction

Section Part G - Errors and Complaints

66. Errors
66.3. Relevant error
66.7. Serious Error
67. Complaints

APPENDIX

A: List of Authorising Officers

PART A Introduction & RIPA General

1. Introduction

1.1 The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of undercover officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) governs these activities and provides a means of ensuring that they are carried out in accordance with law and subject to safeguards against abuse.

All surveillance activity can pose a risk to the Council from challenges under the HRA or other processes. Therefore, it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Council's processes, procedures and oversight responsibilities.

In preparing this policy the Council has followed the RIPA Codes of Practice (August 2018), Office of Surveillance Commissioners (OSC) Procedures and Guidance 2016 (still current).

If having read this document you are unclear about any aspect of the process, seek advice from Legal Services.

2. Scope of Policy

2.1 The purpose of this Policy is to ensure there is a consistent approach to the undertaking and authorisation of surveillance activity that is carried out by the Council. This includes the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS). This will ensure that the Council complies with RIPA .

2.2 This document provides guidance on the authorisation processes and the roles of the respective staff involved.

2.3 The policy also provides guidance on surveillance which is necessary to be undertaken by the authority but cannot be authorised under the RIPA legislation. This type of surveillance will have to be compliant with the Human Rights Act (see section 3 below).

2.4 The policy also identifies the cross over with other policies and legislation, particularly with the Data Protection Act and the Criminal Procedures Act.

2.5 All RIPA covert activity will have to be authorised and conducted in accordance with this policy, the RIPA legislation and Codes of Practice. Therefore, all officers involved in the process will have regard to this document and the statutory RIPA Codes of Practice issued under section 71 RIPA (current versions issued in August 2018) for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). The Codes of Practice are available from:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

3. Background to RIPA and Lawful Criteria

3.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force making it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR).

3.2 Article 8 of the European Convention on Human Rights states that: -

1) Everyone has the right of respect for his private and family life, his home and his correspondence.

2) There shall be no interference by a Public Authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

3.3 The right under Article 8 is a qualified right and Public Authorities can interfere with this right for the reasons given in 3.2 (2) above if it is necessary and proportionate to do so.

3.4 Those who undertake Directed Surveillance or CHIS activity on behalf of a Local Authority may breach an individual's Human Rights, unless such surveillance is **lawful,** consistent with Article 8 of the ECHR and is both **necessary** and **proportionate** to the matter being investigated.

3.5 RIPA provides the legal framework for lawful interference to ensure that any activity undertaken, together with the information obtained, is HRA compatible.

3.6 However, under RIPA, Local Authorities can now only authorise Directed Surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment; (serious crime criteria) or involves the sale of alcohol or tobacco to children.

3.7 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 6 months imprisonment.

3.8 Furthermore, the Council's authorisation can only take effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).

3.9 RIPA ensures that any surveillance which is undertaken following a correct authorisation and approval from a Justice of the Peace is lawful. Therefore, it protects the authority from legal challenge. It also renders evidence obtained lawful for all purposes.

4. Consequences of Not Following RIPA

4.1 Although not obtaining authorisation does not make the authorisation unlawful per se, it does have some consequences: -

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own claim on Human Rights grounds i.e. we have infringed their rights under Article 8;
- If a challenge under Article 8 is successful, the Council would receive reputational damage and could face a claim for financial compensation;
- The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC)
- It is likely that the activity could be construed as an error and therefore have to be investigated and a report submitted by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO).

5. Independent Oversight

5.1 RIPA was overseen by the Office of Surveillance Commissioners (OSC). However, from 1 Sept 2017 oversight is now provided by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.

5.2 They have unfettered access to all locations, documentation and information systems as is necessary to carry out their full functions and duties and they will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

5.3 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information they require for the purpose of enabling them to carry out their functions. Therefore, it is important that the Council can show it complies with this Policy and with the provisions of RIPA.

PART B Surveillance, Types and Criteria

6. Introduction

6.1 It is important to understand the definition of surveillance; what activities are classed as surveillance and the different types of surveillance covered by RIPA and the HRA. Surveillance can be both overt and covert and, depending on their nature, are either allowed to be authorised under RIPA or not. There are also different degrees of authorisation depending on the circumstances.

7. Surveillance Definition

7.1 **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.

8. Overt Surveillance

8.1 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 of the Data Protection Act.

9. Covert Surveillance

9.1 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.

9.2 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);

10. Intrusive Surveillance

10.1 Rushmoor Borough Council has no authority in law to carry out Intrusive Surveillance. Only the Police and other law enforcement agencies can lawfully carry out intrusive surveillance.

10.2 Intrusive surveillance is defined in section 26(3) of the 2000 Act as 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 is carried out by means of a surveillance device.

10.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

10.4 A risk assessment of the capability of equipment being used for surveillance on residential premises and private vehicles, such as high-powered zoom lenses, should be carried out to ensure that its use does not meet the criteria of Intrusive Surveillance.

11. Directed Surveillance Definition

11.1 The Council can lawfully carry out Directed Surveillance, providing the Lawful Grounds (set out below in paragraph 14 below) are satisfied. Surveillance is Directed Surveillance if the following are all true:

- It is covert, but not intrusive surveillance;

- It is conducted for the purposes of a specific investigation or operation;

- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);

- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

12. Private information

12.1 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the

environment they are in at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

12.2 The Code of Practice provides guidance on what is private information. They state private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

12.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a Public Authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

12.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a Directed Surveillance authorisation may be considered appropriate.

12.5 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a Directed Surveillance authorisation is appropriate.

12.6 Information which is non-private may include publicly available information such as, books, newspapers, journals, TV and radio broadcasts, newswires, websites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

12.7 There is also an assessment to be made regarding the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance.

13. Confidential or Privileged Material

13.1 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material

contains confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed Surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be authorised by the Chief Executive.

13.2 **Advice should be sought from Legal Services if there is a likelihood of obtaining this type of material.**

14. Lawful Grounds

14.1 As mentioned earlier the Lawful Grounds for Directed Surveillance is a higher threshold for Local Authorities and cannot be granted unless it is to be carried out for the purpose of preventing or detecting a criminal offence(s) and it meets the serious crime test i.e. that the criminal offence(s) which is sought to be prevented or detected is

1) Punishable, whether on summary conviction or on indictment, by a maximum term **of at least 6 months of imprisonment**, or,

2) Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (see 1.4 above). This is the only ground available to the Council and hence the only justification.

14.2 Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

15. Test Purchases

15.1 Test purchase activity does not in general require authorisation as a Covert Human Intelligence Source (CHIS) (for further information on CHIS, see Part C) 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.

15.2 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 (Sec 245 OSC Procedures & Guidance 2016).

16. Urgent cases

16.1 As from 1 November 2012 there is no provision to authorise urgent oral authorisations under RIPA for urgent cases as all authorisations have to be approved by a J.P. If surveillance is required to be carried out in an urgent situation or as an immediate response, this would have to be justified as necessary and proportionate under HRA. This type of surveillance is surveillance outside of RIPA. Please contact Legal Services for advice and consideration of the lawfulness and proportionality of such surveillance.

17. Surveillance for Preventing Disorder

17.1 Authorisation for the purpose of preventing disorder can only be granted if it involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Surveillance for disorder not meeting these criteria would need to be carried out as surveillance outside of RIPA. (See paragraph 21 below)

18. CCTV

18.1 CCTV is now known as a Surveillance Camera Systems under Section 29(6) Protection of Freedoms Act 2012: "Surveillance camera systems" is taken to include:

> (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems;
>
> (b) any other systems for recording or viewing visual images for surveillance purposes;

This includes

- CCTV;
- Body Worn Video (BWV)
- Automatic Number Plate Recognition;
- Deployable mobile overt mobile camera systems.
- Any other system for recording or viewing visual images for surveillance purposes;
- Any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems; and
- Any other systems associated with, or otherwise connected with those systems.

18.2 The use of the conventional town centre CCTV systems operated by the Council do not normally fall under RIPA. However, it does fall under the Data Protection Act 2018, the Surveillance Camera Code of Practise 2013, issued by the Surveillance Camera

Commissioner, and the Information Commissioner's Office (ICO) 'In the picture: a data protection code of practice for surveillance cameras and personal information'. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

18.3 Operators of the Council's CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

18.4 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, Rushmoor Borough Council's CCTV Code of Practise should be followed where relevant as well as the RIPA Codes of Practice.

18.5 The CCTV staff are to have a copy of the authorisation form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority from the Police, a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the central register for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

18.6 The Surveillance Camera Code of Practice 2013 defines a 'surveillance camera system' as:

- any other systems for recording or viewing visual images for surveillance purposes;
- any systems for storing, receiving, transmitting, processing or checking the images or information obtained.

18.7 This definition will include body worn video (BWV) and overt cameras deployed to detect waste offences such as fly-tipping. This definition has far reaching implications as the use of any cameras that meet the requirement will have to be used in a manner that complies with the codes of practice mentioned above and the Data Protection Act.

19. Automatic Number Plate Recognition (ANPR)

19.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle by plotting its locations, e.g. in connection with illegally depositing waste (fly-tipping).

19.2 Should it be necessary to use any ANPR systems to monitor vehicles, the same RIPA principles apply where a Directed Surveillance Authorisation should be sought.

20 Internet and Social Media Investigations

20.1 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.

20.2 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 breeches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

20.3 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.

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

20.5 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.

20.6 There is a detailed separate corporate policy that covers online open source research which should be read and followed in conjunction with this policy (see the Internet & Social Media Research & Investigations Policy).

21. Surveillance Outside of RIPA

21.1 As already explained, for Directed Surveillance the criminal offence must carry **a 6-month prison sentence** or relate to the sale of alcohol or tobacco to children. There are scenarios within an investigation that do not meet this threshold where it may be necessary to undertake surveillance. This will fall outside of RIPA. Examples include:

- Surveillance for anti-social behaviour disorder which do not attract a maximum custodial sentence of at least six months imprisonment.
- Planning enforcement prior to the serving of a notice or to establish whether a notice has been breached.
- Most licensing breaches.
- Safeguarding vulnerable people.
- Civil matters.
- Disciplinary surveillance (see below).

21.2 In the above scenarios they are likely to be a targeted surveillance which are likely to breach someone's article 8 rights to privacy. Therefore, the activity should be conducted in a way which is HRA compliant, which will include a judgement as to whether such surveillance is necessary and proportionate.

21.3 Non RIPA surveillance also includes staff disciplinary surveillance in serious disciplinary investigations. Guidance dictates that this type of surveillance must be compliant with the Monitoring at Work Guidance issued by the Information Commissioner. This is to ensure that is complies with the HRA.

21.4 Should the investigation also involve a criminal offence which meets the RIPA criteria such as fraud, the option to carry out the surveillance under RIPA should be considered. However, it must be a genuine criminal investigation with a view to prosecuting the offender.

21.5 Should it be necessary to undertake disciplinary surveillance advice should be sought from Legal Services.

21.6 As part of the process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed and authorised by an Authorising Officer. A copy of the non RIPA surveillance application form can be obtained from the RIPA Co-Ordinator.

21.7 The SRO will therefore maintain an oversight of non RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The RIPA Co Ordinator will maintain a central record of non RIPA surveillance.

21.8 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- General observations as per section 3.33 in the codes of practice that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the officer will overtly respond to the situation.

- Use of overt CCTV and Automatic Number Plate Recognition systems.

- Surveillance where no private information is likely to be obtained.

- Surveillance undertaken as an immediate response to a situation.

- Covert surveillance not relating to criminal offence which carries a maximum sentence of 6 months imprisonment or relate to the sale of alcohol or tobacco to children (this is likely to be surveillance outside of RIPA).

- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence.

- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear.

In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.

22. Joint Agency Surveillance

22.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.

22.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Co Ordinator. This will assist with oversight of the use of Council staff carrying out these types of operations. Line Managers should be made aware if their staff are involved in this type of surveillance.

23. Use of Third-Party Surveillance

23.1 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not themselves a Public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party conducts which meet the RIPA definitions of Directed Surveillance should be authorised. This is because the agent will be subject to RIPA in the same way as any employee of the Council would be. The Authorising Officer should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required, please contact Legal Services.

23.2 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a Public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation.

24. Surveillance Equipment

24.1 The Council will maintain a central register of all surveillance equipment such as cameras and noise monitoring devices. This will require a description, Serial Number, and explanation of its capabilities.

24.2 The register will be held and maintained by the RIPA Co-Ordinator. This equipment is available for all departments use.

24.3 All equipment capable of being used for Directed Surveillance such as cameras etc. should be fit for purpose for which they are intended.

24.4 When completing an Authorisation, the applicant must provide the Authorising Officer with details of any equipment to be used and its technical capabilities. The Authorising Officer will have to take this into account when considering the intrusion issues, proportionality and whether the equipment is fit for the required purpose. The Authorising Officer must make it clear on the Authorisation exactly what equipment if any they are authorising and in what circumstances.

25 Communications Data

25.1 Part 3 of the Investigatory Powers Act 2016 replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

25.2 A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD Code of Practice.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

25.3 Finally, the IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

PART C. Covert Human Intelligence Sources (CHIS)

26. Introduction

26.1 RIPA covers the activities of Covert Human Intelligence Sources (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 matters not 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.

26.2 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship. However, Officers must be aware that such information may have been obtained in the course of an ongoing relationship with a family member, friend or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source. How the information was obtained should be established to determine the best course of action. The source and information should also be managed correctly in line with CPIA and the disclosure provisions.

26.3 Recognising when a source becomes a CHIS is therefore important as this type of activity may need authorisation. Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of the contents of this Policy and the CHIS codes of Practice.

26.4 A CHIS, their conduct, and the use to which they are put is defined within Section 26(7) and (8) of RIPA. Chapter 2 of the relevant Code provides examples of where this regime may apply.

26.5 Legal advice should always be sought where consideration is given to the use of CHIS.

27. Definition of CHIS

27.1 Individuals act as a covert human intelligence sources (CHIS) if they:

i) establish or maintain a covert relationship with another person to obtain information.

ii) covertly give access to information to another person, or

iii) disclose information covertly which they have obtained using the relationship or they have obtained because the relationship exists.

27.2 A relationship is established, maintained or used for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. This does not mean the relationship with the Council Officer and the person providing the information, as this is not covert. It relates to how the information was either obtained or will be obtained. Was it or will it be

obtained from a third party without them knowing it was being passed on to the Council? This would amount to a covert relationship.

27.3 It is possible, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes. (Section 2.26 Codes of CHIS Codes of Practice

28. Vulnerable and Juvenile CHIS

28.1 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. 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. Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in his absence, the Deputy Chief Executive).

28.2 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. 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.

28.3 If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult before authorisation is sought as authorisations should not be granted in respect of a Juvenile CHIS unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied.

29. Lawful Criteria

29.1 The lawful criteria for CHIS authorisation is **prevention and detection of crime and prevention of disorder.** The serious crime criteria of the offence carrying a 6-month sentence etc. does not apply to CHIS.

29.2 Authorisations for Juvenile Sources must be authorised by the Chief Executive of the Council (or, in their absence, the Deputy Chief Executive).

30. Conduct and Use of a Source

30.1 The way the Council use a CHIS for covert activities is known as 'the use and conduct' of a source.

30.2 The use of a CHIS involves any action on behalf of a Public Authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.

30.3 The conduct of a CHIS is establishing or maintaining a personal or other relationship with another person for the covert purpose of:

a. Using such a relationship to obtain information, or to provide access to information to another person, or

b. Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship or

c. Is incidental to anything falling within a and b above.

30.4 In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a Public Authority.

30.5 The use of a source is what the Authority does in connection with the source, such as tasking and the conduct is what a source does to fulfil whatever tasks are given to them or which is incidental to it. The Use and Conduct require separate consideration before authorisation. However, they are normally authorised within the same authorisation.

30.6 The same authorisation form is used for both use and conduct. A Handler and Controller must also be designated, as part of the authorisation process (see section 31), and the application can only be authorised if necessary and proportionate. Detailed records of the use, conduct and tasking of the source also have to be maintained.

30.7 Care should be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed (see Section 2.10 of the CHIS Code of Practice)

30.8 Careful consideration must be given to any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS (Section 3.18 of the CHIS Code of Practice)

31. Handler and Controller

31.1 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:

- That there will at all times be an officer (the **Handler**) within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The Handler is likely to be the investigating officer.

- That there will at all times be another officer within the Council who will have general oversight of the use made of the source; **(Controller)** i.e. the line manager.

- That there will at all times be an officer within the Council who has responsibility for maintaining a record of the use made of the source. See CHIS record keeping (see section 37).

31.2 The **Handler** will have day to day responsibility for:

- Dealing with the source on behalf of the Local Authority concerned;
- Risk assessments
- Directing the day to day activities of the source;
- Recording the information supplied by the source; and
- Monitoring the source's security and welfare.
- Informing the Controller of concerns about the personal circumstances of the CHIS that might effect the validity of the risk assessment or conduct of the CHIS

31.3 The **Controller** will be responsible for:

- The management and supervision of the "Handler" and
- General oversight of the use of the CHIS;
- maintaining an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.

32. Undercover Officers

32.1 Oversight and management arrangements for **undercover operatives**, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of the Council. The role of the handler will be undertaken by a person referred to as a **'cover officer'**. (Section 6.9 CHIS Codes of Practice).

33. Tasking

33.1 Tasking is the assignment given to the source by the Handler or Controller such as by asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant Local Authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

33.2 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, Directed Surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

33.3 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

34. Risk Assessments

34.1 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. It is a requirement of the codes that a risk assessment is carried out. This should be submitted with the authorisation request. The risk assessment should provide details of how the CHIS is going to be handled It should also take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

35. Use of Equipment by a CHIS

35.1 If a CHIS is required to wear or carrying a surveillance device such as a covert camera it does not need a separate intrusive or Directed Surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

35.2 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations. This should have been identified at the planning stage.

36. CHIS Management

36.1 The operation will require managing by the Handler and Controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The Authorising Officer should maintain general oversight of these functions.

36.2 During CHIS activity, there may be occasions when unforeseen actions or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and re-authorised (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the Authorising Officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

37. CHIS Record Keeping

37.1 Centrally Retrievable Record of Authorisations

37.2 A centrally retrievable record of all authorisations is held by Rushmoor Borough Council. This record contains the relevant information to comply with the Codes of Practice. These records are updated whenever an authorisation is granted, renewed or cancelled and are available to the Investigatory Powers Commissioner (IPCO) upon request.

37.3 The records are retained for 5 years from the ending of the authorisation.

37.4 Individual Source Records of Authorisation and Use of CHIS

37.5 Detailed records must be kept of the authorisation and the use made of a CHIS. An authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

37.6 The particulars to be contained within the records are;

a. The identity of the source;

b. The identity, where known, used by the source;

c. Any relevant investigating authority other than the authority maintaining the records;

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

e. Any other significant information connected with the security and welfare of the source;

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

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

h. Identity of the Handler and Controller (and details of any changes)

i. The periods during which those persons have discharged those responsibilities;

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

k. All contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

l. The information obtained by each relevant investigating authority by the conduct or use of the source;

m. Any dissemination by that authority of information obtained in that way; and

n. In the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

37.7 The person maintaining these records is the RIPA Co-Ordinator.

37.8 Public authorities are also encouraged to maintain auditable records for individuals providing intelligence who do not meet the definition of a CHIS. This will assist authorities to monitor the status of a human source and identify whether that person should be duly authorised as a CHIS. This should be updated regularly to explain why authorisation is not considered necessary. Such decisions should rest with those designated as Authorising Officers within Public Authorities. (Section 7.5 CHIS Codes of Practice).

37.9. Further Documentation

37.10 In addition to the above, when appropriate records or copies of the following, as are retained by the Council for 5 years:

- A copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;

- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- The reason why the person renewing an authorisation considered it necessary to do so;

- Any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;

- Any risk assessment made in relation to the CHIS;

- The circumstances in which tasks were given to the CHIS;
- The value of the CHIS to the investigating authority;
- A record of the results of any reviews of the authorisation;
- The reasons, if any, for not renewing an authorisation;
- The reasons for cancelling an authorisation; and
- The date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.
- A copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months (where applicable).

37.11 The records kept by the Council should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS (Sec 7.7 CHIS Codes of Practice)

37.12 The relevant application forms are available in the Appendices: https://www.gov.uk/government/collections/ripa-forms--2

References in these forms to the 'Code' are to the Covert Human Intelligence Sources Code of Practice, which should be consulted for further guidance.

PART D. RIPA Roles and Responsibilities

38. The Senior Responsible Officer (SRO)

38.1 The nominated Senior Responsible Officer is Executive Director and Deputy Chief Executive. The SRO has responsibilities for:

- The integrity of the process in place within the Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- Engagement with the Investigatory Powers Commissioner Office (IPCO) and the inspectors who support the Commissioner when they conduct their inspections;

- Where necessary, overseeing the implementation of any recommended post-inspection action plans 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.

39. RIPA Co-Ordinator

39.1 The RIPA Co-Ordinator is the Corporate Manager – Legal Services and is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by the Authorising Officer or refused by a JP.

39.2 The RIPA Co-ordinator will: -

- Keep the copies of the forms for a period of 5 years;

- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and Issue the unique reference number.

- Keep a database for identifying and monitoring expiry dates and renewal dates.

- Along with, Directors, Heads of Service, Authorising Officers, and the Investigating Officers must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Governance Framework, retention schedules and data protection legislation.

- Provide administrative support and guidance on the processes involved.

- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;

- Monitor each department's compliance and act on any cases of non-compliance;

- Provide training and further guidance and awareness of RIPA and the provisions of this Policy; and Review the contents of this Policy.

40. Managers Responsibility and Management of the Activity

40.1 Line Managers within each department of the Council are responsible for ensuring that in all cases where surveillance is required, due consideration is given to the need for covert surveillance before application is made for authorisation. That includes the consideration of using overt action, routine enquiries or inspections which are less intrusive.

40.2 If authorised it is important that all those involved in undertaking Directed Surveillance activities, including Line managers, are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment for the need for the activity to continue including ongoing assessments of the intrusion. All material obtained, including evidence, should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge.

40.3 Line Managers should also ensure that the relevant reviews, renewals and cancellations are completed by the applicant in accordant with the codes and the dates set throughout the process.

41. Investigating Officers/Applicant

41.1 The applicant is normally an investigating officer who completes the application section of the RIPA form. Investigating Officers should think about the need to undertake Directed Surveillance or the use of a CHIS before they seek authorisation and discuss it with their Line manager. Investigating Officers need to consider whether they can obtain the information or achieve their objective by using techniques other than covert surveillance.

41.2 The applicant or some other person must carry out a feasibility study and this should be seen by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form should then be submitted to the Authorising Officer for authorisation.

41.3 The applicant is likely to attend court to seek the approval of a JP. and if approved and involved in the covert activity they must only carry out what is authorised and approved. They, or some other person will also be responsible for the submission of any reviews renewals and cancellations.

42. Authorising Officers

41.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

42.2 Appendix A lists the Authorising Officers within the Council who can grant authorisations all of which are at Service Manager level or above.

42.3 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 must have been trained to an appropriate level so as to have an understanding of the requirements in the Codes of Practice and that must be satisfied before an authorisation can be granted.

42.4 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.

42.5 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.

42.6 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.

42.7 They also need to explain exactly what they are authorising, against who, in what circumstances, where etc. and that the level of the surveillance is appropriate to achieve the objectives. 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.

42.8 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.

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

42.10 Authorised 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. This can be obtained from Legal Services.

43 Necessity

43.1 Obtaining an authorisation under RIPA will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

43.2 The Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds which for Local Authority Directed Surveillance is the

prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco.

43.3 The lawful criteria for CHIS is prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment.

43.4 The applicant and Authorising Officers must also be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there were no other means of obtaining the same information in a less intrusive method. This is a part of the authorisation form.

44. Proportionality

44.1 If the activities are deemed necessary, the Authorising Officer must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

44.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

44.3 When explaining proportionality, the Authorising Officer should explain why the methods and tactics to be adopted during the surveillance is not disproportionate.

44.4 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

- 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 will cause the least possible intrusion on the subject and others;

- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

45. Collateral Intrusion

45.1 Before authorising applications for Directed Surveillance, the Authorising Officer should also take into account the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance.

45.2 Staff should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. 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.

45.3 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.

45.4 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 Act requirements.

45.5 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.

45.6 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.

45.7 Where a Public Authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

PART E. The Application and Authorisation Process

46. Relevant Forms

46.1 For both Directed Surveillance and CHIS authorisations there are 4 forms within the process. They are:

- Authorisation
- Review
- Renewal
- Cancellation

46.2 All the forms can be obtained from the Government Website at

https://www.gov.uk/government/collections/ripa-forms--2

47. Duration of Authorisations

47.1 Authorisations must be given for the maximum duration from the Date approved by the JP/Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire, they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a Directed Surveillance authorisation will cease to have effect after three months from the date of approval by the Magistrate unless renewed or cancelled. Durations 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

47.2 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

48. Applications/Authorisation

48.1 The applicant or some other person must carry out a feasibility study and intrusion assessment as this may be required by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form should then be submitted to the Authorising Officer for authorisation.

48.2 When completing an application for authorisation, the applicant must ensure that the case for the authorisation is presented in the application 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 warrant or authorisation. This is a requirement of the codes.

48.3 All the relevant sections must be completed with sufficient information to ensure that applications are sufficiently detailed for the Authorising Officer to consider Necessity, Proportionality having taken into account the Collateral Intrusion issues **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

48.4 If it is intended to undertake both Directed Surveillance and the use of a CHIS on the same surveillance subject, the respective authorisation should be completed and the respective procedures followed. Both activities should be considered separately on their own merits.

48.5 All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation. The form should then be submitted to the Authorising Officer.

48.6 Applications whether authorised or refused will be issued with a unique number (obtained from the RIPA Co-Ordinator) by the Authorising Officer. The number will be taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.

48.7 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Co-Ordinator for recording and filing. If having received the feedback, the applicant feels it is appropriate to re submit the application, they can do so and it will then be considered again.

48.8 Following authorisation, the applicant will then complete the relevant section of the judicial application/order form Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary to and does not replace the need to supply a copy and the original RIPA authorisation as well.

49. Arranging the Court Hearing

49.1 It will be necessary within office hours to contact the administration at the Magistrates' Court to arrange a hearing. The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

49.2 Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the JP. If in doubt as to whether you are able to present the application seek advice from Legal Services.

50. Attending the Hearing

50.1 The applicant will attend the hearing; however, the Authorising Officer should also attend the hearing if required as the applicant can't answer questions directed for the Authorising Officer. Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, the original and a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case. The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

50.2 The JP will read and consider the RIPA authorisation and the judicial application/order form.. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. **However, the forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided.**

50.3 The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation was an appropriate Designated Person within the Council to authorise the activity and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for Directed Surveillance.

51. Decision of the Justice of the Peace (JP)

51.1 The JP has a number of options which are:

51.2 **Approve or renew an authorisation.** If approved by the JP, 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.

51.3 **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.

51.4 Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the JP 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.

51.5 For, a technical error (as defined by the JP), 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.

51.6 **Refuse to approve or renew and quash the authorisation.** This applies where the JP 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 the Legal who will consider whether to make any representations.

51.7 The JP 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.

51.8 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, Legal will decide what action if any should be taken.

51.9 There is a Home Office chart showing the above procedure at https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa. Click on the Guidance for Local Authorities (England and Wales) pdf. For further information or guidance, please contact Legal Service.

52. Post Court Procedure

52.1 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the Authorising Officer is aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Co-Ordinator. A copy will be retained by the applicant and if necessary by the Authorising Officer. The central register will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

52.2 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice and reduce the risk of errors.

53. Reviews

53.1 When an application has been authorised and approved by a JP, regular reviews must be undertaken by the Authorising Officer to assess the need for the surveillance to continue.

53.2 In each case the Authorising Officer should determine how often a review should take place at the outset. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or confidential information. They will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required to ensure that the applicants submit the review form on time.

53.3 Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application which would include a change to the level of intrusion so that the need to continue the activity can be re-assessed. However, if the circumstances or the objectives have changed considerably, or the techniques to be used are now

different, a new application form should be submitted, and it will be necessary to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

53.4 Line mangers of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

53.5 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 to a JP.

53.6 The results of a review should be recorded on the central record of authorisations.

54. Renewal

54.1 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but Directed Surveillance or the use of a CHIS is still required.

54.2 Should it be necessary to renew an authorisation for Directed Surveillance or CHIS, this must be approved by a JP.

54.3 Applications for renewals should not be made until shortly before the original authorisation period is due to expire. However, they must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

54.4 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer for consideration.

54.5 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

54.6 If the Authorising Officer refuses to renew the application, the cancellation process should be completed. If the Authorising Officer authorises the renewal of the activity, the same process is to be followed as mentioned earlier for the initial application whereby approval must be sought from a JP.

54.7 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

55. Cancellation

55.1 The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the Directed Surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

55.2 As soon as the decision is taken that Directed Surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations.

55.3 The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and detail if any images were obtained, particularly any images containing innocent third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc. See sections 58 to 65 Safeguarding and the Use of Surveillance Material below.

55.4 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what was authorised. This check will form part of the oversight function. Where issues are identified including errors , they will be brought to the attention of the Line Manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight and comply with the Codes of Practice.

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

55.6 All cancellations must be submitted to the RIPA Co-Ordinator for inclusion in the central Record and storing securely with the other associated forms.

55.7 Do not wait until the 3 month period is up to cancel. Cancel it at the earliest opportunity when no longer necessary and proportionate. Line Managers should be aware of when the activity needs cancelling and ensure that staff comply with the procedure.

Part F Central Record and Safeguarding the Material

56. Introduction

56.1 Authorising Officers, applicants and Line Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. This includes the legal obligations under the Criminal Procedures and Investigations Act. However, this will not replace the requirements under the Codes of Practice, which includes the fact that the Council must hold a centrally held and retrievable record.

57. Central Record

57.1 The centrally retrievable record of all authorisations will be held and maintained by the RIPA Co-Ordinator. It will be regularly updated whenever an authorisation is applied for, refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from IPCO, upon request.

57.2 All original authorisations and copies of Judicial applications/order forms whether authorised or refused, together with review, renewal and cancellation documents, must be sent within 48 hours to the RIPA Co-Ordinator who will be responsible for maintaining the central record of authorisations. They will ensure that all records are held securely with no unauthorised access. If in paper format, they must be forwarded in a sealed envelope marked confidential.

57.3 The documents contained in the centrally held register should be retained for at five years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater. The centrally held register contains the following information:

- If refused, (the application was not authorised by the AO) a brief explanation of the reason why. The refused application should be retained as part of the central record of authorisation;
- If granted, the type of authorisation and the date the authorisation was given;
- Details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- Name and rank/grade of the authorising officer;
- The unique reference number (URN) of the investigation or operation;
- The title of the investigation or operation, including a brief description and names of subjects, if known;
- Frequency and the result of each review of the authorisation;
- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date renewed by the JP;
- Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- The date the authorisation was cancelled;
- Authorisations by an Authorising Officer where they are directly involved in the investigation or operation. If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

57.4 As well as the central record the RIPA Co-Ordinator will also retain:

- The original of each application, review, renewal and cancellation, copy of the judicial application/order form, together with any supplementary documentation of the approval given by the Authorising Officer;
- The frequency and result of reviews prescribed by the Authorising Officer;

- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the Authorising Officer;
- A record of the period over which the surveillance has taken place. This should have been included within the cancellation form.

57.5 These documents will also be retained for five years from the ending of the authorisation.

58. Safeguarding and the Use of Surveillance Material

58.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through Directed Surveillance or CHIS activity. This material may include private, confidential or legal privilege information. It will also show the link to other relevant legislation.

58.2 The Council should ensure that their 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).

59. Authorised Purpose

59.1 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.

60. Handling and Retention of Material

60.1 As mentioned above, all material associated and obtained with an application will be subject of the provisions of the Data Protection Act (DPA) 2018 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.

60.2 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.

60.3 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.

60.4 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.

60.5 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.

60.6 If retention is beyond these periods it must be justified under DPA. 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.

61. Use of Material as Evidence

61.1 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.

61.2 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.

61.3 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.

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

62. Dissemination of Information

62.1 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 in section 59 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.

62.2 The obligations apply not just to this 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 Rushmoor Borough 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.

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

63. Storage

63.1 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.

64. Copying

64.1 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.

64.2 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.

65. Destruction

65.1 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.

Part G. Errors and Complaints

66. Errors

66.1 Errors can have very significant consequences on an affected individual's rights. Proper application of the surveillance and CHIS provisions in the RIPA codes and this Policy should reduce the scope for making errors.

66.2. There are two types of errors within the codes of practice which are:

- Relevant error and
- Serious error.

66.3 Relevant Error

66.4 An error must be reported if it is a "**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 would include compliance by public authorities with Part II of the 2000 Act (RIPA). This would include with the content of the Codes of Practice.

66.5 Examples of relevant errors occurring would include circumstances where:

- Surveillance 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 Surveillance Codes of Practice relating to the safeguards of the material.

66.6 All relevant errors made by Public Authorities must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report no later than ten 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 analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

66.7 Serious Errors

66.8 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 they consider 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.

66.9 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

67. Complaints

67.1 Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Borough Solicitor who will investigate the complaint. A complaint can also be made to the official body which is the Investigatory Powers Tribunal (IPT). They have jurisdiction to investigate and determine complaints against any Public Authority's use of RIPA powers, including those covered by this Policy.

67.2 Complaints should be addressed to:

The Investigatory Powers Tribunal

PO Box 33220

London

SWIH 9ZQ