APPENDIX A

RIPA
(The Regulation of Investigatory Powers Act)

CHIS
(Covert Human Intelligence Sources)

COUNCIL POLICY AND GUIDANCE

1. Background

The Regulation of Investigatory Powers Act 2000 (RIPA) provides the legislative framework within which covert surveillance operations must be conducted in order to ensure that investigatory powers are used in accordance with human rights. The Act also regulates the use of confidential human intelligence sources.

The Investigatory Powers Act 2016 sets out the circumstances in which the Council can acquire and use "communications data".

This guidance based on the Home Office Codes of Practice on covert surveillance, covert human intelligence sources and accessing communications data are intended as a practical reference guide for Council officers who may be involved in or are considering covert operations.

They are not intended to replace the Codes of Practice issued by the Home Office and officers involved in covert operations must familiarise themselves with the content of these Codes in order to ensure that they fully understand their responsibilities.

The Codes are available on the web site:
https://www.gov.uk/government/collections/ripa-codes

2. What is covert surveillance?

Covert surveillance is defined in the Act as any 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.

The Act goes on to define two different 'types' of covert surveillance:

a) Directed covert surveillance
b) Intrusive covert surveillance

Intrusive covert surveillance 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.

The Council has no powers to undertake intrusive covert surveillance operations.

3. What is directed covert surveillance?

Directed covert surveillance is defined in the Act as surveillance, which is covert but not intrusive and is undertaken: for the purposes of a specific operation or investigation in such a manner that it is likely to result in the obtaining of private information about a person (whether or not they are the individual specifically identified for the purposes of the operation) 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 for carrying out surveillance

4. For what purposes can the Council conduct directed covert surveillance?

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 specifies that the Council can only use directed covert surveillance for the purpose of preventing or detecting a criminal offence and it meets the conditions set out below:-

The conditions are that the criminal offence which is sought to be prevented or detected is punishable, whether on indictment or summary conviction, by a maximum term of at least six months' imprisonment, or would be an offence under sections;

a) s.146 of the Licensing Act 2003 (sale of alcohol to children);

b) s.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);

c) s.147A of the Licensing Act 2003 (persistently selling alcohol to children);

d) s.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under 18)

If a directed covert surveillance operation does not fall within this purpose the Council may be acting unlawfully under the Human Rights Act. Where an officer is contemplating undertaking surveillance that does not appear to fall within this

purpose and the new conditions as set out above they **must** take advice from the Borough Solicitor.

5. What falls within the definition of directed covert surveillance?

It is safest to assume that any operation that involves planned covert surveillance of a specific person or persons , of however short duration, falls within the definition of directed covert surveillance and will, therefore, be subject to authorisation under RIPA and the amending legislation.

In some circumstances, legitimate surveillance may fall outside RIPA controls. This will be where the surveillance does not relate to the core function of law enforcement, for example in the course of collecting private information for an employment issue. Nonetheless care needs to be taken and the principles behind RIPA should be respected. The Information Commissioner has issued guidance on workplace monitoring. See https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers/

The consequence of not obtaining an authorisation will render the surveillance action unlawful under the Human Rights Act, and/or the evidence obtained inadmissible in any Court proceedings.

It is **the Council's requirement** that Council officers seek an authorisation where the surveillance is **likely** to interfere with a person's Article 8 (Human Rights Act) rights to privacy.

Obtaining an authorisation from the authorised officers and a Magistrate will ensure that the surveillance action is carried out in accordance with the law and is subject to stringent safeguards against abuse. Proper authorisation of surveillance should also ensure the admissibility of evidence under the common law, PACE (Section 78) and the Human Rights Act.

Use of overt (public) CCTV for any covert operation is regulated and governed by the Home Office, the Surveillance Commissioner and Information Commissioner all of which publish detailed information on their websites which should be the source for the latest guidance and best practice.

6. What falls outside of directed covert surveillance?

Anything which constitutes an **immediate response,** e.g. a Council officer with regulatory responsibilities may by chance be present when an individual is potentially infringing the law and it is necessary to observe, follow, or engage in other surveillance tactics as an instant response to the situation to gather further information or evidence. Given the lack of preparation, surveillance in these circumstances is unlikely to be particularly covert.
Once this immediacy has passed, however, any further covert surveillance of the individual should be subject to RIPA authorisation and that of a Magistrate.

7. What is authorisation?

Authorisation is the process by which a directed covert surveillance operation is subject to proper consideration, recording and approval by the officer conducting the investigation and the senior officer authorised to approve it and then obtaining the approval of a Magistrate.
It ensures that all relevant factors have been thoroughly considered and checked. It is also the means by which, in the event of challenge, Council officers can demonstrate that covert surveillance was lawfully conducted and that it is was a fair and reasonable way to proceed, despite the possible intrusion of a person or person's privacy.

Forms in respect of authorisation can be downloaded from the Home Office Website https://www.gov.uk/government/collections/ripa-forms--2 .
Copies of the forms can also be obtained from the RIPA Co-ordinator by emailing dpa@stevenage.gov.uk.

The authorisation forms issued by the Home Office cover all of the necessary aspects. It is important that these forms are correctly and adequately completed for all directed covert surveillance operations.

There is one element of the written application that is of particular importance and is an integral part of a number of the questions contained in the standard application form:

Proportionality - this is a fundamental principle embodied in the Human Rights Act.

Officers must be able to demonstrate that a surveillance operation justifies the level of intrusion of privacy that may occur with regard to the target or targets of the surveillance or any other persons, ***i.e. that it is proportionate set against the outcome.*** We should not use a sledgehammer to crack a nut!

This must be adequately recorded in the application form. It is not enough to simply have a standard phrase saying that the surveillance is proportionate. The rationale for proceeding with covert surveillance needs to be written and explicit. Questions it might be useful to ask to help in framing responses to questions included in the application form are:

- What is the nature of the suspected or alleged offence/infringement?
- What, if any, are the alternatives to covert surveillance, i.e. could the information be reasonably obtained by other means?
- If there are other options why have these been rejected in favour of covert surveillance?
- What is the level of intrusion of privacy likely to be? Minimal? Average? Significant? Interference will not be justified if the means used to achieve the aim are excessive in the circumstances of the case. Further, any proposed interference with a person or people' private, home and family life (HRA Article 8 rights) should be carefully managed and must not be arbitrary or unfair.
- Is legally privileged, personal confidential information or confidential journalistic material likely to be acquired?
- Is the privacy of other persons not connected with the investigation likely to be effected and what steps can be taken to minimise or avoid this? (Collateral intrusion).
- What is the desired outcome?
- What is the anticipated benefit to the Council?

Proportionality in this context has nothing whatsoever to do with whether or not the possible benefit of a covert surveillance operation justifies the time and money expended by the Council.

Authorising Officers are required to further consider the proportionality of any proposed surveillance and may challenge assumptions or statements that do not appear to provide adequate justification.

In making an application, the case for the warrant or authorisation should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which support or weakens the case for the warrant or authorisation;

8. Who can authorise surveillance operations and how to complete an application?

The Protection of Freedoms Act 2012 amended the RIPA 2000 Act to make all Local Authority authorisations subject to judicial approval.

The Council has to have all its RIPA surveillance authorisations (that is, use of directed surveillance and covert human intelligence sources) **approved by a designated officer AND a magistrate** before they take effect.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010/521specifies the officers who can authorise RIPA applications.

Stevenage Borough Council designates the following officers for authorising RIPA applications: Strategic and Assistant Directors only (**See RIPA management structure at Appendix A)**

There are 4 key steps to making an RIPA application:

i. Apply to the Data Protection Team for a Unique reference number (URN) and to obtain a copy of the RIPA authorisation application form by emailing dpa@stevenage.gov.uk. The form can also be downloaded directly from the Home Office website at https://www.gov.uk/government/collections/ripa-forms--2
ii. Sumit application form to Authorising Officers for approval and signature via the RIPA Co-ordinator
iii. Contact the RIPA Co-ordinator & Borough Solicitor to apply to Magistrate for approval at Stevenage Magistrates Court: https://courttribunalfinder.service.gov.uk/courts/stevenage-magistrates-court
iv. The original signed authorisation and all supporting documents must be passed to the Data Protection Team for filing and recording at dpa@stevenage.gov.uk

9. What is the role of the Authorising Officer?

The Authorising Officer is the officer who takes responsibility for the instigation of the surveillance activity. It is therefore important that:

- The Authorising Officer has undertaken training in relation to their role as an authorising officer under RIPA; and
- The Authorising Officer exercises careful and independent judgment in deciding whether or not to authorise, giving a full statement of their reasons for authorisation. This is not a rubber-stamping exercise and the Authorising Officer may be called upon to defend their decision.

10. Special authorisation requirements for “sensitive” information

Where there is likelihood that legally privileged, personal confidential information or confidential journalistic material will be acquired as a result of a directed covert surveillance operation authorisation must be made by the Chief Executive (or Deputy) as the Senior Responsible Officer (SRO), (see RIPA management structure chart at Annex A below), and then by a Magistrate.

11. What is legally privileged information, private or confidential information or confidential journalistic material?

Definition of legal professional privilege, private information, confidential information and confidential journalistic material

Legal professional privilege

"legal professional privilege" means matters to which the following applies;

(1) communications between a professional legal adviser and-
(a) his client, or (b) any person representing his client,
which are made in connection with the giving of legal advice to the client.
(2) communications-
(a) between a professional legal adviser and his client or any person representing his client, or (b) between a professional legal adviser or his client or any such representative and any other person, which are made in connection with or in contemplation which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

(3) items enclosed with or referred to in communications of the kind mentioned in (1) or (2) and made-
(a) in connection with the giving of legal advice, or
(b) in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

Exclusions -
(a) communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and
(b) communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

Private information

“private information” means-

Any information relating to an individual’s private or family life, and should be taken generally to include any aspect of a person’s private or personal relationship with others including family and professional or business relationships

Confidential information

This covers: a) confidential personal information (b) confidential constituent information and (c) confidential journalistic material.

Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner/ Inspector during their next inspection and the material be made available if requested.

Confidential personal information means:

Information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on

disclosure or an obligation of confidentiality contained in existing legislation. For example a consultation between a doctor and a patient.

Confidential constituent information means:

Information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Confidential journalistic material means:

Material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from Shared Legal Services before any further dissemination of the material takes place.

12. What is the duration of authorisations?

Authorisation for a directed covert surveillance operation will cease to have effect (unless renewed) at the end of a period of **3 months** beginning with the day on which it took effect.

Authorisation for a directed covert surveillance operation using a human intelligence source will cease to have effect (unless renewed) at the end of a period of **twelve months** beginning with the day on which it took effect. It is good practice to keep authorisations under regular review. Do not simply rely on the passage of time for expiry to take place.

13. How is an operation reviewed, renewed or cancelled?

All covert operations or investigations must be effectively assessed and regularly monitored by the officer conducting the operation and the authorising

officer. The authorisation process should be viewed as a useful management tool to help officers to achieve this.

Reviews

Regular reviews of authorisations should be undertaken at least monthly to assess the need for surveillance to continue. Responsibility for assessing the appropriate review period rests with the authorising officer and this should be as frequently as considered necessary and practicable. All reviews should include a re-examination of the **necessity** and **proportionality** of the authorisation, and its impact; e.g. whether there is a greater level of collateral intrusion than anticipated.

There is clear guidance on reviews, renewals and cancellations in the Home Office Codes of Practice and officers should refer to the appropriate sections for further details. The standard review, renewal and cancellation forms issued by the Home Office cover all the necessary aspects with copies of all related forms available from the Data Protection Team. It is important that these forms are correctly and adequately completed.

Renewals

NB. All applications for renewals have be approved by a magistrate

In addition applications for renewal will record:

Whether this is the first renewal, if not, every occasion on which the authorisation has previously been renewed;

The reason why it is necessary to continue with the surveillance;
The content and value to the investigation or operation of the information so far obtained by the surveillance;

The results of regular reviews of the investigation or operation.

Cancellation

An authorising officer who granted or last renewed an authorisation **must** cancel it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was originally authorised.

Even if an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled.

14. What is a covert human intelligence source (CHIS)?

A person is a CHIS if:

They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the two bullet points below;

- They covertly use such a relationship to obtain information or to provide access to information to another person; or

- They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

15. What is likely to fall within the definition of a CHIS for Council purposes?

The use of CHIS's by the Council is likely to be extremely rare. This type of source of information will be more commonly used by the Police, Security Service, Customs & Excise, other intelligence services etc. where it is normal practice to use agents, informants and officers working undercover.

The "use" of a source involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

There are occasions, however, when the Council may use a CHIS to obtain information, e.g.

A CHIS may be used as a source to obtain information in respect of an investigation into housing or Council Tax benefit fraud; this may be a Council officer acting undercover.

A CHIS may be used as a source to obtain information in respect of an investigation into the loss of monies at Council premises where there are cashier activities; this may be a Council officer acting undercover.

This list is clearly not definitive. There is an element of judgement involved in determining when an individual taking some part in an investigation may be acting as a CHIS and the matter is not entirely black and white.

A member of the public volunteering a piece of information to the Council regarding something they have witnessed in their neighbourhood is not a CHIS. They are not passing information obtained as a result of a relationship which has been established or maintained for a covert purpose. However, if the Council asks them to use a relationship to gather further information, then they may need to be treated as a CHIS. An investigating officer conducting covert investigations on social media using a covert identity (i.e.an alias) may become a CHIS if s/he establish a relationship with the account user.

A duty of care to the individual should always be considered and a special caution exercised if the person could be at risk of reprisals if the information is acted on.

In all cases where consideration is given to use of a CHIS, please take advice from Legal Services.

16. Special requirements to observe when using a CHIS?

There are rules about the use of vulnerable adults or juveniles as sources and There are also special requirements with regard to the management, security and welfare of sources. For further details refer to the sections detailed above in the Home Office CHIS Code of Practice.

The same requirements of necessity and proportionality exist for the granting of these authorisations as are set out for directed surveillance.

Additionally the authorising officer shall not grant an authorisation unless they believe that arrangements exist for the source's care which satisfies the following requirements:-

There will at all times be an officer with day to day responsibility for dealing with the source and the source's security and welfare;
There will be at all times an officer who will have general oversight of the use made of the source;
There will at all times be an officer with responsibility for maintaining a record of the information supplied by the source;
Records which disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available;
All CHIS authorisations must contain or have attached a risk assessment.

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age). On no account can a child under 16 years of age be authorised to give information against his or her parents. Similar safeguards also apply to the use of vulnerable individuals as sources. (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 herself, or unable to protect himself or herself against significant harm or exploitation.)

Vulnerable or juvenile CHIS may only be authorised by Assistant Directors or whoever deputises in their absence. Further advice must be sought from Legal Services before using juveniles or vulnerable individuals as sources, to ensure that all necessary legal requirements are complied with.

There are also specific legal rules which must be followed in relation to the management of sources. Details are given in the relevant Home Office Code of Practice, and further advice can be obtained from Legal Services.

17. Social Media Investigations

Some investigations that use the internet may meet the criteria of directed surveillance. Especially if a profile is built by processing data about a specific individual or group of individuals without their knowledge. There is a fine line

between general observation, systematic observation and research and it is unwise to rely on a perception of a person's reasonable expectations or their ability to control their personal data.

The internet is deemed a surveillance device under RIPA, as surveillance is covert "if, and only if, it is conducted in a manner that is calculated to ensure that persons subject to the surveillance are unaware that it is, or may be taking place.

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

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

If an officer strikes up a covert social media relationship for the purpose of an investigation, e.g. by becoming a "friend" on Facebook, they may be acting as a CHIS and this needs to be properly authorised in advance.

Officers using the internet for investigations should refer to paragraphs 3.10 - 3.17 of the Revised Code of Practice for specific guidance on determining when RIPA authorisation is required. The Code of Practice can be found at: CHIS Code (publishing.service.gov.uk). Officers should also refer to the Social Media Evidence Log Template under Appendix A, where using social media to obtain evidence.

For further advice on the use of social media and RIPA, please contact the Shared Legal Services team.

18. Accessing Communications Data

In accordance with Part 3 of The Investigatory Powers Act, 2016, local authorities can authorise **the acquisition and disclosure of 'communications data' provided that the acquisition of such data is necessary for the purpose of preventing or detecting crime or preventing disorder**; and proportionate to what is sought to be achieved by acquiring such data.

19. What is 'Communications data'?

Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 261 of the Act and falls into three main categories: -

Traffic data – where a communication was made from, to whom and when

Service data – use made of service e.g. Itemised telephone records

Subscriber data – information held or obtained by operator on person they provide a service to.

Local authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

NB. Nothing permits the interception of the content of any communication

20. Who can authorise communication data applications?

Only the Head of the Shared Legal Services (Borough Solicitor or deputy) can apply for and authorise these applications and acts as the Councils' single point of contact (SPOC) for these applications.

The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and as before, final approval has to be given by a Magistrate.

Officers requiring communication data authorisation should consult the Borough Solicitor for advice and assistance.

21. Records, equipment and monitoring

A central record of all authorisations must be held. This register will be securely held by the RIPA Co-ordinator. Register information will be held for **a period of five (5) years**.

Officers should refer to the appropriate sections of the Codes of Practice detailed above for guidance on the maintenance and retention and destruction of authorisation records that are held in addition to the register.

Material obtained through directed or intrusive surveillance, or entry on, or interference with, property or wireless telegraphy, 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, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 198470 and the Human Rights Act 1998.

Officers should be particularly mindful of the provisions of the Criminal Procedure and Investigation Act and the Code of Practice issued under it. This Code of Practice provides guidance on the recording, retention and disclosure of material acquired during the course of an investigation. The Code of Practice can be found at: Criminal Procedure and Investigations Act Code of Practice - GOV.UK (www.gov.uk)

Where the product of surveillance or property interference could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In the case of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996, which requires that the investigator retain all material obtained in an investigation which may be relevant to the investigation.

22. Training

Due to the speciality of the training requirements for RIPA and CHIS investigations, external accredited specialist companies should be sourced to provide training to ensure officers, including authorising officers, receive the most up to date requirements, techniques and advice on best practice.

23. General Advice and Oversight

The RIPA Co-ordinator maintains the central register of authorisations and is available to advise generally on questions regarding surveillance, and guidance to senior officers in signing/review of applications. The RIPA Co-ordinator is the Records & Information Governance Manager, who can be contacted by emailing dpa@stevenage.gov.uk

The RIPA Co-ordinator will provide assistance and guidance with the application to Magistrates and Court procedure and be responsible for liaison with the Investigatory Powers Commissioner's Office and the implementation of any recommendations.

24. Errors

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. 58.2 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.

There are two types of errors within the Codes which are: "relevant error" and "serious error".

(a) Relevant Error An error must be reported if it is a 'relevant error'. A relevant error is any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This includes compliance by the Council with RIPA and the content of the Codes. 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 relating to the safeguards of the material

All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report provided 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.

(b) Serious Errors The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless 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 HRA) is not sufficient by itself for an error to be a serious error.

25. Complaints

Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Council in accordance with the Council's Corporate Complaints Procedure.

Any person may also make a complaint to the official body, which is the Investigatory Powers Tribunal (IPT), about the Council using covert techniques against them. Details explaining how to make a complaint can be found on the IPT's website. The IPT has jurisdiction to investigate and determine complaints against the Council's use of RIPA powers, including those covered by this Policy.

Complaints to the IPT should be emailed to: info@ipt-uk.com or posted to: The Investigatory Powers Tribunal PO Box 33220 London SWIH 9ZQ

26. Legislation and other sources of information and guidance

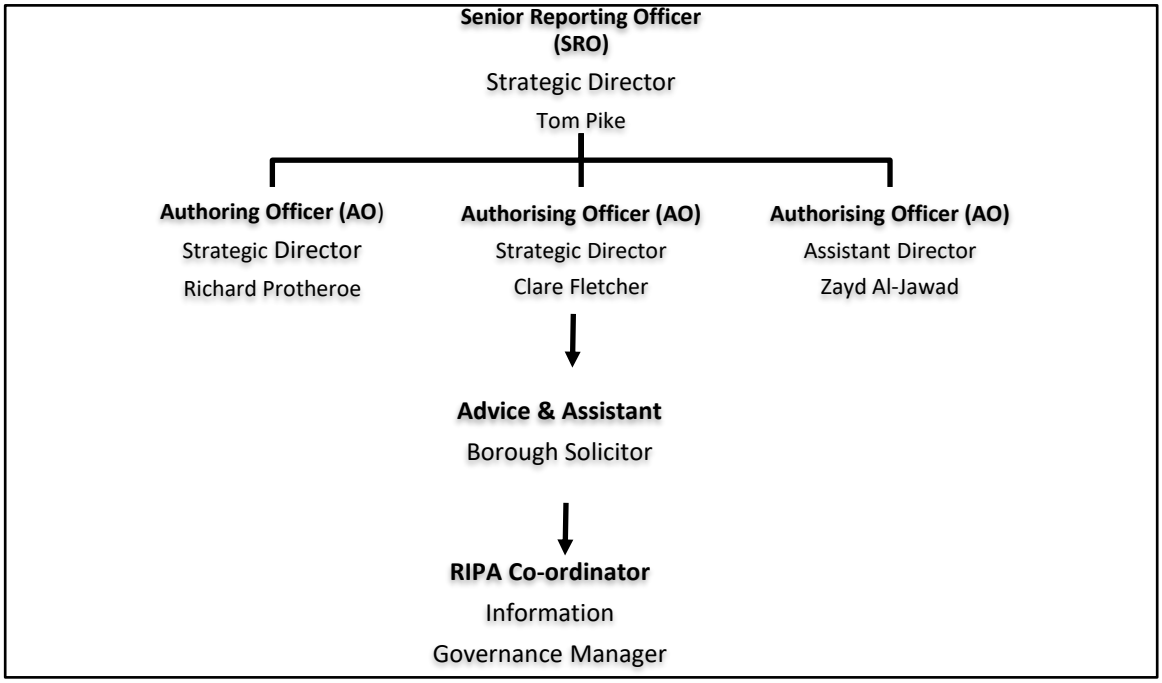
Legislation: http://www.legislation.gov.uk/ukpga/2000/23/contents

a) **The Regulation of Investigatory Powers Act 2000 (RIPA);**
b) **The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521 (the 2010 order);**
c) **The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 (the 2012 order);**
d) **The Protection of Freedoms Act 2012.**
e) **The Investigatory Powers Act 2016**

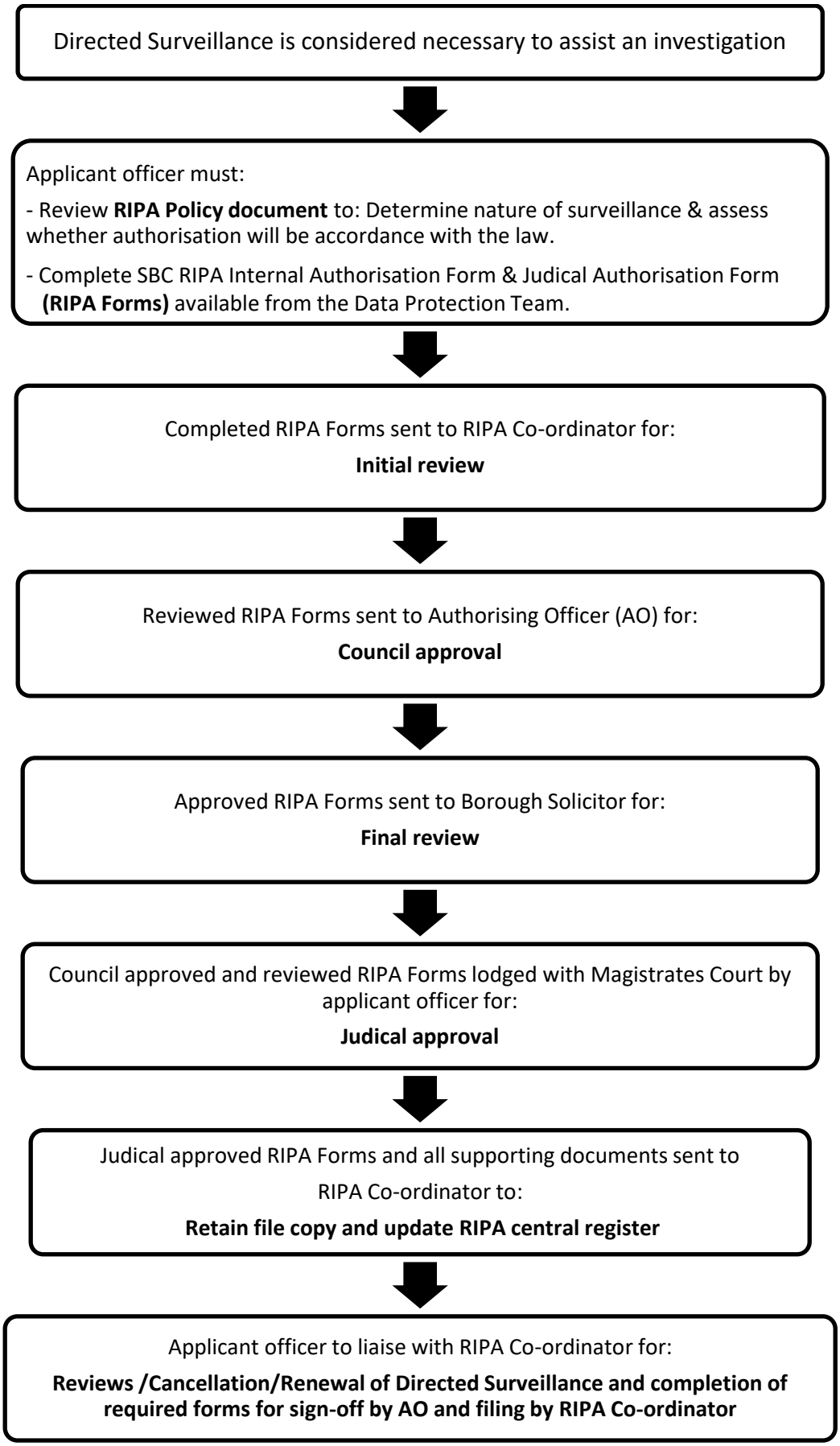
The Home Office - https://www.gov.uk/search?q=ripa

Investigatory Powers Commissioner's Office - IPCO – Investigatory Powers Commissioner's Office

APPENDIX A RIPA MANAGEMENT STRUCTURE



RIPA PROCESS FLOWCHART



SOCIAL MEDIA - EVIDENCE LOG TEMPLATE

Investigating officers should use this log template to record all evidence obtained using social media to ensure the Council meets its RIPA Records and Product Management requirements, that covers the retention, review and destruction of any evidence obtained through use of covert powers.

Date Evidence obtained	Media platforms/ sites visited as part of the investigation (e.g. google maps, Meta, X, etc)	What evidence has been obtained?	Is obtained evidence considered necessary and proportionate to achieve objectives of the surveillance? Please provide reasons. (Where obtained evidence is not considered necessary to achieve objectives, it should be securely destroyed/disposed, otherwise evidence to be retained for 5 years from authorisation cancellation date.)	Is evidence to be retained or disposed? (Where evidence is retained, it should be held securely by applicant officer within the relevant service team for the required 5 year retention period. - Where evidence is to be disposed, please confirm method and date of disposal.)