Employees' Guide

Regulation of Investigatory Powers Act 2000

Directed Surveillance and Use of Covert Human Intelligence Sources

				Ref. Number	FP 78
Authorised By	Allan Oldfield	**Job title**	Chief Executive	**Issue Date**	Dec 2014
Author	Ian Curtis			**Revision No**	**Jun 2022**
End users of hard copies of this document are responsible for ensuring their copy is up to date.					

Revised June 2022

1 Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

1.2 Fylde Council is therefore included within the RIPA framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources.

1.3 The purpose of this guidance is to:

- explain the scope of RIPA and the circumstances where it applies
- provide guidance on the authorisation procedures to be followed.

1.4 The Council has had regard to the Code of Practice produced by the Home Office in preparing this guidance. It is available on the Internet at www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice.

1.5 This policy is reviewed annually by the full council. Additionally, reports on the use of authorisations under RIPA are made to the council's Audit and Standards Committee on a quarterly basis.

1.6 In summary RIPA requires that when the Council undertakes directed surveillance or uses a covert human intelligence source, these activities must satisfy certain conditions and be authorised by an officer with delegated powers and approved by a Justice of the Peace.

1.7 The authorising officers for the council are the chief executive and the deputy chief executive.

1.8 There are special rules that apply where the Council intends to undertake directed surveillance or use a covert human intelligence source and the surveillance or use of the source is likely to result in confidential material or privileged material being acquired. In those circumstances, the chief executive must authorise the use of the source. Nobody else can authorise the surveillance or use of the source unless the chief executive is absent.

1.9 The same special rules apply where the council intends to use a covert human intelligence source who is under 18 years old, or who is vulnerable. A person is vulnerable if he or she 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. Again, the chief executive must authorise the use of such a source. Nobody else can authorise the surveillance or use of the source unless the chief executive is absent.

1.10 The council will only use a person who is vulnerable as a covert human intelligence source in the most exceptional circumstances, and will not use any person who is under 16 years old.

1.11 Authorisation and approval under RIPA gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation and approval helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention on Human Rights which is now enshrined in English law through the Human Rights Act 1998. This is because any interference with the private life of citizens will be "in accordance with the law". Provided activities undertaken are also "reasonable and proportionate", they will not be in contravention of Human Rights legislation.

1.12 It should be noted that the Council cannot authorise Intrusive Surveillance. Investigators should familiarise themselves with the provisions of chapters 5 and 6 of the Code of Practice on Covert Surveillance to ensure a good understanding of the limitation of powers within RIPA.

1.13 Deciding when authorisation is required involves making a judgment. Paragraph 2 sets out some factors you will need to consider. If you are in any doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Head of Governance. While it is always safer to get authorisation, many kinds of investigation may not involve the use of the kinds of surveillance covered by RIPA.

1.14 The Head of Governance has responsibility for maintaining a centrally retrievable record of authorisations under RIPA and for overseeing:

1.14.1 the integrity of the process in place within the authority to authorise and seek approval of directed surveillance;

1.14.2 compliance with Part II of the 2000 Act, Part III of the 1997 Act and with the codes of practice;

1.14.3 engagement with the Investigatory Powers Commissioner's Office ("IPCO") and inspectors when they conduct their inspections, and

1.14.4 where necessary, overseeing the implementation of any post-inspection action plans.

1.15 Before any officer of the Council undertakes or commissions any surveillance of any individual or individuals they need to assess whether the activity comes within RIPA. In order to do this the following key questions need to be asked.

2 Directed Surveillance

2.1 What is meant by Surveillance?

"Surveillance" includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

2.2 When is surveillance directed?

Surveillance is 'Directed' for the purposes of RIPA if it is covert and is undertaken:

a) for the purposes of a specific investigation or a specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and

c) 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 the carrying out of the surveillance.

2.3 Is the surveillance covert?

Covert surveillance is that carried out in a manner **calculated** to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the RIPA framework will normally not apply.

2.4 Is it for the purposes of a specific investigation or a specific operation?

For example, are Town Hall CCTV cameras which are readily visible to anyone walking around the building covered?

The answer is not if their usage is to monitor the general activities of what is happening in the car park. If that usage, however, changes, RIPA may apply.

For example, **if** the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific operation. However, the operation will only require authorisation if the surveillance is covert.

2.5 Is it in such a manner that is **likely** to result in the obtaining of private information about a person?

"Private information" is any information relating to a person's private or family life.

An investigation that merely gathers intelligence about a person's use of public spaces and premises open to the public would not by itself usually be likely to result in the obtaining of private information.

For example, the fact that a person has visited a particular pub and spoke to another particular person on a particular occasion will not be private information about either of them. But recording information about what they talk about may be. Private information may also be obtained if several records about what the person did in a public place are analysed together to produce a pattern of behaviour.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside RIPA framework. However, the use of 'test purchasers' may involve the use of covert human intelligence sources (see later). If in doubt, speak to your Authorising Officer.

2.6 Otherwise than by way of an immediate response to event or circumstances where it is not reasonably practicable to get authorisation

The Home Office gives the example of an immediate response to something happening during the course of an observer's work, which is unforeseeable.

However, if as a result of an immediate response, a specific investigation subsequently takes place that brings it within RIPA framework.

2.7 Is using the internet or social media to get information about in individual directed surveillance?

The internet and social media can be valuable resources for investigations. If you use the internet or social media just to identify individuals who might be of interest, you will probably not be doing directed surveillance and would not have to obtain RIPA authorisation. But if you are using them to build up a more complete picture of someone's behaviour and habits, you might need to consider obtaining an authorisation.

The key consideration is whether you are getting private information. If you are only using information you could get the information by casual browsing, that is not likely to be private information. But if you are visiting a site or feed multiple times, or combining information from a number of online sources, to help you with your investigation of an individual, the position may be different. You be carrying out directed surveillance and need an authorisation. The former Office of Surveillance Commissioners issued guidance on when the use of social media and the internet might need authorisation under RIPA. You can read the guidance at appendix 4. You can also look at paragraphs 3.10 to 3.17 of the Code of Practice.

3 Is the Surveillance Intrusive?

3.1 Surveillance becomes intrusive if it:

a) is carried out in relation to anything taking place on any **residential premises** or in any **private vehicle**; and

b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or

c) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it 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.

3.2 Surveillance is also automatically deemed to be intrusive if it relates to certain kinds of premises which are, at the time of the surveillance, being used for legal consultations. The premises are prisons, courts, police stations, legal practitioners' offices and high security hospitals.

The council cannot carry out intrusive surveillance.

4 Covert use of Human Intelligence Source (CHIS)

4.1 A person is a Covert Human Intelligence Source if:

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c),

b) he covertly uses such a relationship to obtain information or provide access to any information to another person; or

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

4.2 A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

4.3 An example of a CHIS would be an officer or other person who pretends to form a friendship with a suspect, but who is really using that relationship to secretly obtain information from the suspect.

4.4 It would be unusual for the council to use a CHIS, but if you do so, you need to obtain authorisation

5 Authorisations, approvals, renewals and cancellations

5.1 The Process for Authorisation and Approval

5.1.1 Obtaining authorisation and approval is a two-stage process. The first stage is to obtain authorisation from an Authorising Officer. Details of Authorising Officers and their remits are in paragraphs 1.7 to 1.10.

5.1.2 The second stage is to obtain approval from a Justice of the Peace. This involves applying to the magistrates' court. The council will follow the Home Office guidance on applying for approval. Only qualified lawyers or officers authorised by the council under section 223 of the Local Government Act 1972 can make the application for approval and appear in court.

5.1.3 A Justice of the Peace, in considering giving approval to an authorisation, must consider whether the statutory tests have been met and whether the use of the surveillance technique is necessary and proportionate.

5.1.4 An authorisation or renewal is not effective until it has been approved by a Justice of the Peace. The investigating officer should not begin the authorised surveillance until it has been approved.

5.2 The Conditions for Authorisation

5.2.1 *Directed Surveillance*

5.2.1.1 For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

a) that an authorisation is **necessary** for the purpose of preventing or detecting crime or of preventing disorder and

b) the authorised surveillance is **proportionate** to what is sought to be achieved by carrying it out.

5.2.1.2 In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such the forms listed in the Appendix are to be completed where relevant.

5.2.1.3 Authorisations should provide enough flexibility to avoid the need for amendments to accommodate minor changes in the times or methods of surveillance, while still facilitating effective monitoring of compliance with the authorisation.

5.2.2 *Covert Use of Human Intelligence Sources*

5.2.2.1 The same principles apply as for Directed Surveillance. (see paragraph 5.1.1 above), but there are some additional requirements. The person authorising use of a CHIS must believe that management arrangements for the source satisfy requirements laid down in RIPA and relevant regulations. The requirements are set out in Appendix 3.

5.2.2.2 The conduct so authorised is any conduct that:

a) is comprised in any such activities involving the use of a covert human intelligence source, as are specified or described in the authorisation;

b) relates to the person who is specified or described as the person to

whose actions as a covert human intelligence source the authorisation relates; and

c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

5.2.2.3 In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such the forms listed in appendix 2 are to be completed where relevant.

5.2.2.4 It is also sensible to make any authorisation sufficiently wide enough to cover all the means required, while still facilitating effective monitoring of compliance with the authorisation.

5.3 Requirements of RIPA

5.3.1 All authorisations **must** be in **writing**. The Appendix to this guidance refers to standard forms, which must be used. **Officers must direct their mind to the circumstances of the individual case with which they are dealing when completing the form.**

5.3.2 Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a source.

5.3.3 Authorisations lapse, if not renewed, three months from the date of approval by the Magistrates Court for directed surveillance and twelve months from date of approval by the Magistrates Court for the conduct or use of a covert human intelligence source. **Nevertheless, the authorising officer must ensure that each authorisation specifies an expiry date**.

5.3.4 The person who originally granted the authorisation can renew it in the same terms at any time before it ceases to have effect. If the person who originally granted the authorisation is unavailable, another person entitled to grant a new authorisation can renew it. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation. Any renewal will not be effective unless approved by the Magistrates Court.

But, for the conduct of a covert human intelligence source, an Authorised Officer should not renew unless a review has been carried out and that person has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

5.3.5 The benefits of obtaining an authorisation are described in paragraph 7 below.

5.4 Factors to Consider

5.4.1 Any person giving an authorisation should first satisfy him/herself that the authorisation is **necessary** on particular grounds and that the surveillance is **proportionate** to what it seeks to achieve. This will include consideration of the guidance in paragraphs 3.3 to 3.6 of the Covert Surveillance and Property Interference Code of Practice.

5.4.2 Particular consideration should be given to **collateral intrusion** on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of especial concern in cases where there are special sensitivities, for example in cases of premises used for any form of medical or professional counselling, advice or therapy.

5.2.8 An application for an authorisation should include **an assessment of the risk** of any collateral intrusion or interference. The authorising officer must take this into account when considering the proportionality of the surveillance.

5.4.3 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

5.4.4 Any person giving an authorisation will also need to be aware of particular **sensitivities in the local community** where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. Where the Authorising Officer considers that conflicts might arise they should consult a senior police officer before granting the authorisation.

5.5 Home Surveillance

5.5.1 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance at his/her home, or where there are special sensitivities.

5.6 Spiritual Counselling

No operations should be undertaken in circumstances where investigators believe

that surveillance would lead to them intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, absolution of conscience or counselling concerning appropriate repentance. "Minister of Religion" does not necessarily imply a paid office.

5.7 Confidential Material

5.7.1 RIPA does not provide any special protection for confidential material. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under this guidance.

5.7.2 In general, any application for an authorisation that is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

5.7.3 The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Head of Governance before further dissemination takes place;

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Head of Governance) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

- Confidential material should be destroyed as soon as it is no longer

necessary to retain it for a specified purpose.

5.8 Combined authorisations

A single authorisation may combine two or more different authorisations under RIPA. Combined authorisations must not include intrusive surveillance activity.

5.9 Partnership working

The council's human resources service and fraud investigation services are outsourced to other councils. As the tasking authority, it is Fylde's responsibility to provide the authorisation. This means that where the outsourced human resources or fraud investigation service wishes to carry out directed surveillance or use a CHIS, authorisation must be obtained from an appropriate Authorising Officer of Fylde Council. An authorisation sought or granted by an officer of the council providing the outsourced service would not be valid under RIPA and would not give lawful authority for the activity.

6 Handling and disclosure of product

6.1 Control of material

6.1.1 Material acquired through covert surveillance or the use of a CHIS will always be personal information. This means that it must be handled in accordance with data protection laws. Fylde Council will be the data controller for all material produced in an operation authorised on the application of Fylde Council, regardless of whether it is physically in the possession of Fylde or of a partner organisation. The paragraphs below set out the procedures for handling material.

6.1.2 If the procedures allow the material to be shared or given to another person or body, that person or body must agree to comply with the procedures equivalent to those set out below. They must also agree not to share or give any of the material to any other person or body. If the other person or body does not agree, the material should not be shared or given to them unless Fylde Council's data protection officer has agreed in writing.

6.2 Copying

6.2.1 Except as mentioned below, you should not make copies of any material unless needed for the purposes of the investigation it forms part of, any other investigation that it is relevant to, or legal proceedings connected with them. Apart from this, you can only make copies for certain statutory purposes. "Making copies" includes not only copying the whole of the material, but also making extracts summaries or records which identify themselves as the

product of the surveillance or CHIS.

6.2.2 You should not send any material via email or any other method of transmission which is not secure, even within Fylde Council.

6.3 Storage

6.3.1 If the material is digital, you must store it in a password protected file, and must not disclose the password to any other person. Under no circumstances should any material be kept in a shared drive or put on a memory stick or other storage device, unless it is required to be disclosed as part of any legal procedure, in which case it must be password protected.

6.3.2 If material is held as hard copy, it must be secured and locked in such a way that no person not concerned with the investigation has access to it.

6.4 Destruction

6.4.1 Material must be destroyed once it is no longer needed. Material is deemed to be no longer needed five years after the earliest of the following has happened: (a) any legal proceedings in which the material is part of the evidence, or is unused information, have concluded (including the conclusion of any appeal) and the material is not needed in connection with any other ongoing or contemplated legal proceedings; (b) a decision has been made to not proceed with legal proceedings in connection with the operation for which the material was obtained and the material is not needed in connection with any other ongoing or contemplated legal proceedings; or (c) a review as contemplated by 6.4.2 below has concluded that there is no material possibility of the material being used in any legal proceedings.

6.4.2 Any stored material should be reviewed by the officer in charge of the investigation for which it was obtained no later than one year after it was obtained, and subsequently at intervals of no more than one year to decide whether there is a realistic possibility of it being used in any legal proceedings.

6.4.3 There is nothing in RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, you should always bear in mind that the purpose of your surveillance is governed by its authorisation. If the purpose changes, you will need to seek a new authorisation.

7 The Use of Covert Human Intelligence Sources

7.1 The Authorising Officer must consider the continuing safety and welfare of

any employee to be used as a CHIS, and the foreseeable consequences to others of the tasks they are asked to carry out. He should assess any risk to the employee **before** authorisation is given.

7.2 The Council's practice is **not** to use an employee acting as a source to infiltrate existing criminal activity, or to be a party to the commission of criminal offences, even where this is within the limits recognised by law.

7.3 The Authorising Officer must believe that the use of an employee as a source is proportionate to what it seeks to achieve. He should satisfy himself that the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use of the source seeks to achieve. Accurate and proper records should be kept about the source and tasks undertaken.

7.4 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, confidential material is likely to be obtained.

8 Confidential material

RIPA does not provide any special protection for confidential material. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the relevant Home Office Code. In general, any application for an authorisation that is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired.

9. Central Register of Authorisations

9.1 RIPA requires a central register of all authorisations to be maintained. The Head of Governance or his nominated representative maintains this register.

9.2 Whenever an authorisation is granted the Authorising Officer must arrange for the following details to be forwarded by e-mail to the Head of Governance or nominated representative. Receipt of the e-mail will be acknowledged.

- Whether it is for Directed Surveillance or CHIS ;
- Applicants name, job title and directorate;
- Applicant's address and Contact Number;
- Identity of 'Target';
- Authorising Officer and Job Title; (in line with delegation scheme)
- Date of Authorisation;
- Whether the special provisions for urgent authorisation were used and, if so, why;

- Whether the investigation or operation is likely to result in obtaining confidential material; and
- The first date for review.

A copy of the authorisation should be sent either with the notification or to follow as soon as practicable afterwards.

9.3. The Head of Governance or person nominated to maintain the register of authorisations will:

a) Review the authorisation and draw the authorising officer's attention to any issues or problems with it;

b) Check that arrangements have been made to seek approval of the authorisation from the Magistrates Court and to forward details of the approval for inclusion on the central record when granted;

c) Remind authorising officers of the expiry of authorisations;

d) Check that surveillance does not continue beyond the authorised period;

e) At the anniversary of each authorisation, remind authorising officers to consider the destruction of the results of surveillance operations;

f) At the fifth anniversary of each authorisation, remind authorising officers to consider destruction of the forms of authorisation, renewal or cancellation.

9.4 It is each director's responsibility to securely retain all authorisations, renewals and cancellations within their directorate. These records are confidential and should be retained for a period of five years from the ending of the authorisation. Once the investigation is closed (bearing in mind court proceedings may be lodged some time after the initial work) the records held by the directorate should be disposed of in an appropriate manner (e.g. shredded).

10 Cancellation of authorisations [moved from elsewhere in the Guide]

10.1 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 5.2.9.3 above.

10.2 Authorising Officers are responsible for ensuring that authorisations undergo

timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary. It is good practice for a cancellation application to describe the activity undertaken, any material acquired and how that material is to be managed.

10.3 Authorising Officers must ensure that the relevant details of each authorisation are sent to the designated officer for registration as described in paragraph 8 above.

6.4 The authorised officer should retain applications for directed surveillance for 5 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

11 Benefits of Obtaining Authorisation under RIPA.

11.1 Authorisation of surveillance and human intelligence sources

RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and

- the conduct is in accordance with the authorisation, **then**

- it shall be "lawful for all purposes".

However, the corollary is not true – i.e. if you do **not** obtain RIPA authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits.

11.2 RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which -

a) is incidental to any conduct that is lawful by virtue of authorisation; and

b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question

12 Scrutiny and Tribunal

IPCO regulates conduct carried out under RIPA. The Commissioner provides independent oversight of the use of investigatory powers by intelligence agencies, police forces and other public authorities. This includes authorising directed surveillance and the use of covert human intelligence sources.

APPENDIX 1.

Definitions from RIPA

- **"Confidential Material"** consists of:

  a) matters subject to legal privilege;
  b) confidential personal information; or
  c) confidential journalistic material.

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing hi/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below)

- **"Confidential Personal Information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  a) to his/her physical or mental health; or
  b) to spiritual counselling or other assistance given or to be given, and

  which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office (see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

c) it is held subject to an express or implied undertaking to hold it in confidence; or

d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- "**Confidential Journalistic Material"** includes 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.

Note A. *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.*

Note B. *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

APPENDIX 2.

1. RIPA 2000 PART II **APPLICATION** FOR AUTHORITY FOR DIRECTED SURVEILLANCE

2. RIPA 2000 PART II APPLICATION FOR **RENEWAL** OF DIRECTED SURVEILLANCE

3. RIPA 2000 PART II APPLICATION FOR **CANCELLATION** OF DIRECTED SURVEILLANCE

4. RIPA 2000 PART II **REVIEW** OF DIRECTED SURVEILLANCE

5. RIPA 2000 PART II APPLICATION FOR **CHANGE OF CIRCUMSTANCES** OF DIRECTED SURVEILLANCE

APPENDIX 3

Management arrangements for CHIS

[From RIPA, section 29(5)]

a) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have day-to-day responsibility for dealing with the source on behalf of that authority, and for the source's security and welfare;
(b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the source;
(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the source;
(d) that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and
(e) that records maintained by the relevant investigating authority that 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 to those persons.

The matters specified in paragraph (d) are the following (see The Regulation of Investigatory Powers (Source Records) Regulations 2000)
:

(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) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
(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.

APPENDIX 4

Covert surveillance of Social Networking Sites (SNS)

[From paragraph 289, OSC Procedures and Guidance 2016]

289 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation for directed surveillance where private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).