Peterborough City Council

Regulation of Investigatory Powers Act

Policy

Document Control

Purpose of document:	The approach to the use of RIPA powers and the process followed by Peterborough City Council when these powers are used
Intended audience:	Officers who may use directed covert surveillance as part of an investigation
Type of document:	Policy and procedure
Document lead/author	Ben Stevenson, Data Protection Officer
Other documents that link to this one:	RIPA toolkit on Insite
Document ratified/approved by:	Audit Committee
Version number:	Version 1.2
Issue date:	June 2018
Dissemination method:	Notification to staff via the Weekly Round-up newsletter and via All Staff notifications on the front page of Insite.
Date due for review:	March 2019
Reviewer:	Director of Legal and Governance

DOCUMENT REVISION RECORD:

Description of amendments:	Version No.	Date of re-approval and re-issue
Review in light of legislation and procedural changes	2	March 2015
Document control added. Review in light of inspection and changes in officers	3	June 2018

Introduction

The Regulation of Investigatory Powers Act 2000 ('RIPA') regulates covert investigations by a number of bodies, including local authorities.

The Revised Codes of Practice for use of such powers provide guidance to understand when RIPA applies and the procedures to follow. The Protection of Freedoms Act 2012 placed restrictions on when a local authority can use RIPA powers.

Authorisation under RIPA by one of the Council's Authorised Officers gives authority to carry out Covert Surveillance, acquire communications data and use Covert Human Intelligence Source.

Authorisation ensures that the powers conferred by RIPA are used lawfully and in a way that does not interfere with the surveillance subject's Human Rights. It also requires those authorising the use of covert techniques to give proper consideration to whether use is necessary and proportionate.

The purpose of this Corporate Policy and Procedures Document is to explain:

- the scope of RIPA and the circumstances where it applies; and
- the authorisation procedures to be followed following the Protection of Freedoms Act 2012

Key Role Definitions

Senior Responsible Officer – the Senior Responsible Officer (SRO) provides senior management oversight of the use of RIPA and provides assurance that the appropriate statutory controls are in place.

Our SRO is Fiona McMillan, Director of Legal & Governance.

Central Monitoring Officer (CMO) – the CMO will maintain the central registers for covert surveillance and communications data and is responsible for coordinating of training, updates of policies, procedures and inspections.

Our CMO is Ben Stevenson, Data Protection Officer.

Authorising Officer (RIPA) – an authorising officer must be of service manager or above rank and will consider the application made under RIPA. They will consider the information

provided by the applicant and determine whether there is necessity and proportionality in authorising the surveillance request.

For a list of authorising officers, please see Appendix 2.

Applying Officers – whether the application falls under RIPA, an applying officer is responsible for completing the application in full and providing sufficient details for the Authorising Officer to consider the application. The applying officer must never be the authorising officer.

Useful Websites

General Guidance from the Investigatory Powers Commissioner's Office

Home Office guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance

RIPA Forms

Code of Practice- Surveillance, Covert Human Intelligence and Acquisition and Disclosure of Communications Data

Basic determination of RIPA

It is critical that prior to any activity being undertaken, an officer and an authorising officer undertake an assessment of the activity proposed.

This assessment should follow the procedure as detailed below.

Question	Answer	Notes
1. Is the surveillance activity covert?	Yes – proceed to question 2	This means that a subject is unaware of the activity due to the way it being undertaken
2. Is the surveillance directed?	Yes – proceed to question 3	This means that the activity is for a specific investigation or purpose
3. Is the investigation into a criminal offence?	Yes – proceed to question 4	If it is not an investigation the alleged commission of a criminal offence then RIPA does **not** apply however you should always be able to show that you have considered whether RIPA does apply.
4. Are you likely to obtain confidential or private information	Yes – proceed to 5	If you are not likely to obtain such information then RIPA does not apply.
5. Does the offence meet the crime threshold?	If yes then RIPA applies	If it does not then RIPA does **not** apply however you should always be able to show that you have considered whether RIPA does apply.

Please refer to Surveillance Checklist

Covert Surveillance

What is Surveillance?

Surveillance includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device.

When is surveillance covert?

Surveillance is covert when it is carried out in a manner calculated to ensure that the subject or others affected by the surveillance are unaware that it is or may be taking place.

RIPA regulates two types of covert surveillance namely directed and intrusive.

When is surveillance directed?

Surveillance is 'Directed' (Revised Codes of Practice paragraph 2.2) if it is covert and undertaken:

- 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 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 under Part II of the 2000 Act to be sought.

When is Surveillance Intrusive?

THE COUNCIL IS NOT AUTHORISED TO CARRY OUT INTRUSIVE SURVEILLANCE

Surveillance is intrusive, (Revised Codes of Practice paragraph 2.11) if it is covert and:

- 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 or surveillance device in the premises or in the vehicle.

N.B. Surveillance which 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 is not intrusive unless 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.

The Surveillance Checklist

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

Is the Surveillance Covert?

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

If activities are open and not hidden from the subject of an investigation, RIPA does not apply. Conversely if it is hidden, consider whether surveillance is likely to be directed or intrusive.

Is it Directed?

This means whether or not it is for the purpose of a specific investigation or a specific operative. The use of surveillance for general purposes will not normally be 'directed' and will not therefore require RIPA authorisation. An example of this is the use of CCTV cameras for general area wide observation. *However,* if the surveillance is used as a means of targeting a specific person or persons then RIPA will apply if private information is likely to be obtained. In such circumstances Officers should also be mindful of the possibility of collateral intrusion (see pages 8 – 9) when applying for the appropriate authority.

Private Information

The 2000 Act states that private information includes any information relating to a person's private or family life. Private information 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.

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.

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.

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.

If it is unlikely that observations will result in the obtaining of private information about a person then it is outside RIPA.

Is the crime threshold met?

The Protection of Freedoms Act 2012 introduced a *crime threshold* for local authorities wishing to carry out directed surveillance.

This means that local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment,

- by a maximum term of at least 6 months' imprisonment **or**
- are related to the underage sale of alcohol and tobacco as per article 7A of the 2010 Order.

A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low level offences such as littering, dog control and fly posting.

If the offence changes during an investigation and meets the threshold test, then an application may be made.

Is it proportionate?

In determining whether the activity is proportionate, paragraph 3.4 of the Revised Codes of Practice, the following must be considered:

- Have we balanced the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Have we explained how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- have we considered whether the activity is an appropriate use of the
- legislation and a reasonable way, having considered all reasonable

alternatives, of obtaining the necessary result;

- have we evidenced, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

When surveillance falls outside of RIPA?

There will occasions when a council officer undertakes activity which does not meet the criteria of RIPA. Any activity whether governed by RIPA or not should be undertaken with clear consideration whether it is necessary and proportional to the objectives. It is incumbent on every officer to consider this prior to engaging in any kind of surveillance.

Given the potential for challenge by a subject during legal proceedings, it is the council's policy that such actions will still be governed by the RIPA framework to the extent that an officer must show that they have considered whether RIPA applies. This should be done by the using the Basic RIPA Determination at the start of this policy or Appendix 9 Checklist as an aide to the officers – this is an ongoing process for any investigation. It may be formalised during file reviews by managers, supervision meetings, prior to interviews or prior to the consideration of any legal proceedings. A manager or head of service should ensure that activities have followed the correct procedure.

Surveillance which can termed overt does not require authorisation – a visit to a property with the intention to speak to the occupier would not constitute surveillance. If there is no intention to speak to the occupier such as "drive pasts" to obtain information then this may become surveillance and therefore this policy applies. One visit to the property to obtain the details of a vehicle will not be considered surveillance however repeated visits to establish a pattern of behaviour will be considered and the appropriate form will be required.

CCTV

Peterborough City Council operates a CCTV system which can be used in surveillance where appropriate and where authorised. The corporate code of practice is available and covers the use by Police and non-Police agencies.

Peterborough City Council has an agreed protocol with Cambridgeshire Police which is held by the CMO and CCTV Manager.

Covert Use of Human Intelligence Source ("CHIS")

The Revised Codes of Practice (paragraph 2.1) state that a person is a Covert Human Intelligence Source if:

(a) they establish or maintain 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) they covertly use such a relationship to obtain information or to provide access to any information to another person; or

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

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.

Authorisation is not required where members of the public volunteer information to the Council as part of their normal civic duties or to contact numbers set up to receive information (e.g. a Housing Benefit Fraud hotline).

The Council can only use a CHIS if authorisation has been authorised and received judicial approval. Authorisation will only be give if the use of the CHIS is for the purpose of preventing or detecting crime or of preventing disorder.

Before use of a CHIS is authorised, advice must be sought from the Senior Responsible Officer or their appointed deputy.

The Conditions for Authorisation

Covert Directed Surveillance

For covert directed surveillance an Authorising Officer will not grant an authorisation unless he/she believes (and the prescribed forms require that the factors below are shown to have been taken into account):

(a) that an authorisation is necessary; and

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

An authorisation is necessary if:

(a) The offence is punishable by a maximum term of six months imprisonment on conviction or is related to the underage sale of alcohol and tobacco as per article 7A of the 2010 Order.

An authorisation will be proportionate if the person granting the authorisation has balanced the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

(a) necessary for the ground stated above; and

(b) proportionate to its aim.

In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. The prescribed forms (held by the Authorising Officer) must be fully completed.

It is also sensible to make any authorisation sufficiently wide enough to cover all that is required. This will also enable effective monitoring of what is done against that authorised. The use of stock phrases or cut and paste narrative should be avoided at all times to ensure that proper consideration is given the particular circumstances of each case.

Particular consideration should be given to collateral intrusion or interference with the privacy of persons other than the subject(s) of surveillance and wherever possible steps should be taken to avoid or minimise it. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy, or in a particular community.

Any application for authorisation should include an assessment of risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the surveillance.

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.

The applying officer should also undertake a surveillance assessment which includes a health and safety risk assessment, Appendix 8.

Judicial approval should then be sought. The corporate procedure for this can be found in Appendix 6.

See also Other Factors to be taken into account in certain circumstances.

Use of Covert Human Intelligence Sources

The same necessary grounds and proportionate principles apply but the crime threshold does not apply in this area.

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.

In order to ensure that an Authorising Officer has sufficient information to make an informed decision the prescribed forms (held by the Authorising Officer) must be fully completed. Advice must have also been sought from the Senior Responsible Officer prior to the consideration of authorisation.

It is also sensible to make any authorisation sufficiently wide enough to cover all that is required. This will also enable effective monitoring of what is done against that authorised.

The Authorising Officer must consider the safety and welfare of the source person acting as a Covert Human Intelligence Source and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the start, for the safety and welfare of the source person, even after cancellation of the authorisation, needs to be considered.

The Authorising Officer must believe that the authorised use of the source person as a Covert Human Intelligence Source is proportionate to what it seeks to achieve. Accurate and proper records should be kept about the tasks undertaken.

The applicant, and the Authorising Officer if required, will attend to obtain judicial approval. The corporate procedure can be found at Appendix 6.

The Applicant will have day-to-day responsibility for dealing with the source person and for the source person's security and welfare. They will be termed the **handler.** They will have responsibility for

- Dealing with the CHIS on behalf of the authority
- Directing the day to day activities of the CHIS
- Recording the information supplied by the CHIS
- Monitoring the CHIS's security and welfare

A senior manager, not the Authorising Officer, will at all times have general oversight of the use made of the source person and maintaining a record of such use. They will be termed the **controller** in accordance with the codes of practice. They will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

The senior manager will need to comply with the Regulation of Investigatory Powers (Source Records) Regulations which requires that certain records be kept relating to each source. Each Authorising Officer has a copy of the aforesaid Regulations.

Use of social media in investigations

The use of the internet and its content such as social media such as Facebook, Instagram and Twitter is an investigation is permitted. In accessing such sites, officers must consider the issues of privacy and collateral intrusion.

Even though a person may have placed information about themselves or others in the public arena, they have done so with an expectation of a degree of privacy. Viewing information on the internet may constitute covert surveillance, particularly if there is monitoring of subjects involved for example to establish patterns of behaviour.Appendix 10 may assist officers in assessing whether their actions can be considered to be surveillance.

If an investigating officer enters into a 'conversation' with a profile, and the officer informs them that he is contacting them in his role as an employee of the council, then this contact will be overt and no authorisation will be required.

Where the activity does not include monitoring of material in the public domain, RIPA will not apply. If repeated visits to a site are made then this will constitute monitoring and consideration needs to be given to the use of social media or the internet as part of that in

investigation.

“Public setting”

If an investigating officer views for example a Facebook profile with whom they are not ‘friends’ which is not protected by any privacy settings the information can be treated as being in the public domain. Any initial viewing/visiting of this profile will be overt and authorisation under RIPA will not be required.

If the officer frequently or regularly views the same individual’s profile this is considered targeted surveillance and a RIPA authorisation is required should it meet the stated RIPA test in this policy. If it does not then the officer should be able to show that they have considered whether RIPA applied.

Using a covert identity

Where officers are building and maintaining a relationship with an individual without that individuals knowing the true nature for the purposes of an investigation, this will require an application for the use of a CHIS. This will include where an officer sends a friend request for example. Officers must not create a false identity to establish a profile. The agreed process for the use of a CHIS is detailed above.

Officers must not use their own accounts for work purposes nor for any form of surveillance.

Any use of the internet in an investigation must be fully documented, using Appendix 10.

Application and Authorisation Process

Should the criteria be met, an officer will need to submit a directed surveillance application form to an authorising officer. The application form must be the latest version available on the Home Office website to ensure we are using the most up to date.

All sections relevant to the application must be completed and in a manner in which any authorising officer can understand i.e. it is not necessary for the authorising officer to be a specialist in the applicant’s area.

The application must contain the following information

- A description of the investigation to date include details of the alleged offence which meets the crime threshold , details of subjects involved and an intelligence evaluation
- The conduct to be authorised must be described in detail
- Assessments of the local area, health and safety and risk have been completed
- Confirm the purpose of the operation and what it hopes to achieve
- What the operation will entail e.g. static, mobile, use of cameras.

- Where it will take place, when and how long will it last, remembering to be proportionate
- A description of what information will be obtained and how this will assist the investigation
- Explain why the directed surveillance is necessary i.e. it meets the crime threshold
- Explain the potential for collateral intrusion, why it is unavoidable and how it will be minimised.
- Explain how this is proportionate to what it seeks to achieve.
- Explain whether there is the likelihood of obtaining confidential information as defined by the codes of practice. This must be answered yes or no – stating that it is unlikely will not be accepted as this suggests it remains a possibility

This application should be submitted to the Authorising Officer to consider.

An authorising officer must review each case on its merits and explain why they authorise the conduct, considering necessity and proportionality along with any collateral intrusion.

Prior to seeking judicial approval, the application must be submitted to the CMO who will allocate a unique reference number. The corporate procedure for obtaining judicial approval should be adhered to. The CMO must be notified of the outcome and provided with a copy of the approval/refusal supplied.

Combined or Joint Services

As the Council works with its partner agencies such as Cambridgeshire Police or Cambridgeshire Fire and Rescue then consideration must be given to who makes the application and authorise. In a joint operation, one agency must be assigned as the lead and will obtain authorisation. If it is not the Council, we will still record this activity and ensure that our central record reflects this.

In instances where it is a joint or shared service, the appropriate lead authority must make the application with due regard for the governance arrangements at partner authorities.

Paragraph 3.17 of the Codes of Practice advises that where possible, public authorities should seek to avoid duplication of authorisations as part of a single investigation or operation. For example, where two agencies are conducting directed or intrusive surveillance as part of a joint operation, only one authorisation is required. Duplication of authorisations does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities.

If the Council is tasked to undertake the surveillance on behalf of another agency then that agency should obtain authorisation. Council officers should ensure that they clearly understand the the precise nature of what has been authorised to ensure that they comply. Council officers must only undertake surveillance activity in line with this policy and the limitations of activities placed on local authorities by the Protection of Freedoms Act 2012.

Combined Authorisations

In line with Codes of Practice paragraph 3.12, a single authorisation may combine two or more different authorisations under RIPA however the provisions applicable for each of the authorisations must be considered separately by the appropriate authorising officer. It does not preclude the obtaining of separate authorisations .

Lapse of Authorisations

Authorisation should not be allowed to lapse. They should be reviewed and cancelled or renewed. However the legal position with regard to lapse is as follows:-

WRITTEN - Covert Human Intelligence Source - 12 months from the date of the approval of a magistrate or last renewal.

WRITTEN - Directed Surveillance – 3 months from the date of approval of a magistrate or last renewal.

Renewal of Authorisations

A Magistrate will be responsible for renewing an existing authorisation in the same terms at any time before it ceases to have effect.

However, for the conduct of a Covert Human Intelligence Source, an Authorising 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. The renewal must be receive judicial approval.

Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

Retention Period for Authorisations

Authorisations (together with the Application reviews, renewals and cancellation) should be retained by the Authorising Officer, for a period of 3 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. It is each department's responsibility to securely retain all authorisations within their departments.

Reviews of Authorisations

Regular review of authorisations should be undertaken to assess the need for the surveillance/CHIS to continue. The results of the review need to be sent for recording on the Central Register.

Cancellation of Authorisations

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied the authorisation no longer meets the criteria upon which it was authorised. No authorisation should be left to simply expire.

The process for cancellation is for the investigating officer to submit the cancellation form to the Authorising Officer. This cancellation should detail the reason for cancellation, the benefits or issues arising of the operation and any outcome. It should also include the time spent on the operation. A copy of this form must be forwarded to the CMO to retain on the central record.

Immediate response to situations

The ability for a local authority to grant urgent oral authorisation for use of RIPA has been removed. It is recognised that council officers find themselves in a situation where they need to carry out some form of surveillance without the time to complete a form and obtain authorisations. In these instances, the officer should obtain authorisation from their line manager and also record their reasons, actions, what was observed and be prepared to explain their decisions.

Other Factors

Spiritual Counselling

No operations should be taken in circumstances where investigators believe that surveillance will lead to them intruding on spiritual counselling between a Minister and a Member of his/her faith. In this respect, spiritual counselling is defined as conversations with Minister of Religion acting in his-her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

Legally Privileged and Confidential Material

RIPA does not provide any special protection for 'confidential material'. (Revised Codes of Practice paragraph 4.1) Nevertheless, such material is particularly sensitive, and is subject to additional safeguards (see also Appendix 1). In cases where the likely consequence of the conduct of a Covert Human Intelligence Source would be for any person to acquire knowledge of confidential material, the deployment of the Covert Human Intelligence Source should be subject to consultation with the Chief Executive and Senior Responsible Officer.

In general, any application for an authorisation which 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.

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. If there is doubt as to whether the material is confidential, advice should be sought from the Head of Legal Services 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 Principal Lawyer) is satisfied that it is necessary for a specific purpose;

The retention of 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. This should only be with the approval of the Chief Executive and Senior Responsible Officer.

Data Protection

Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, It should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

RIPA does not prevent material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the Council, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained requires authorisation by the Director of Legal and Governance.

Vulnerable Individuals

The use of a vulnerable individual as a Covert Human Intelligence Source requires authorisation by the Chief Executive or their delegated deputy. The use must always be referred to the Senior Responsible Officer or their deputy for advice prior to authorisation. Such an individual should only be used as a Covert Human Intelligence Source in exceptional circumstances. 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 harm or exploitation.

Community Sensitivities

Officers should always consider whether there are any particular sensitivities within our communities and take these into account if planning surveillance activities in those areas.

Juveniles

The use of a juvenile (under 18) as a Covert Human Intelligence Source requires authorisation by the Chief Executive or their delegated deputy. The use must always be referred to the Senior Responsible Officer or their deputy for advice prior to authorisation

Errors

Any error such as activity undertaken which was not authorised or is conducted beyond the directions of the authorising officer. It will also include failure to declare thorough reviews, renewals, cancellation and poor administration. Any such errors must be reported to the SRO and Central Monitoring Officer.

Central Register of Authorisations

It is a requirement of the revised Code of Practice for Surveillance, paragraph 8.1, that a central register of all authorisations, reviews, renewals, cancellations etc is maintained and regularly updated. The CMO maintains this Register.

It is the Authorising Officer's responsibility to ensure that any application under RIPA is forwarded to the CMO for central registration **within one week of the relevant authorisation, review, renewal, cancellation or rejection.** Each application will be allocated a Unique Reference Number (URN) at this stage and will be monitored by the Compliance Manager to ensure compliance with timescales.

Whenever an authorisation is granted, renewed or cancelled (and this includes authorisations issued by the Police or other third parties using Council CCTV or other facilities) the Authorising Officer must arrange for copies to be forwarded to the CMO. Receipt will be acknowledged.

Codes of Practice

There are Home Office Codes of Practice that expand on this guidance and copies are held by each Authorising Officer. They can be accessed here and officers should ensure that they are consulting the latest version.

The Codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the Codes, “if any provision of the Code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account”.

Benefits of Obtaining Authorisation under RIPA

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".

Acquisition of Communications Data

Communications data means any traffic or any information that is or has been sent via a telecommunications system or postal system, together with information about the use of the system made by any person.

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Companies").

S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a Communications Service Provider is technically unable to collect the data, an authorisation under the section would permit the local authority to collect the communications data themselves.

In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under S22 (4) RIPA must be issued. This must be follow the judicial approval process as outlined in Appendix 5.

The sole ground to permit the issuing of a S22 notice by a Permitted Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Service Provider will most probably have means of collating and providing the communications data requested.

Once a notice has been issued, it must be sent to the Communications Service Provider. In issuing a notice, the Authorising Officer can authorise another person to liaise with the Communications Service Provider covered by the notice.

Application procedure

Should you wish to make an enquiry, contact should be made with the Head of Regulatory Services to consider the request to be made via Trading Standards who have two named authorised officers. The request will be made through NAFN and their process adhered to.

The applicant and authorising officer will need to explain:

- the specific information required with reference to paragraph 3.30 of the codes of practice to streamline the process when dealing with number porting and also to take a more proactive approach to data capture such as top up details when identifying the user of a prepaid mobile.
- why it is relevant
- why it is necessary
- why it is proportionate
- how they will minimise collateral intrusion

A unique reference number should be obtained from the CMO before submission to NAFN. The CMO will record the details.

Once authorised by NAFN, the applicant should follow the procedure for obtaining judicial approval.

Training

There will be a bi-annual programme of training for officers, which may include face to face or e-learning training. Refresher training will be provided on a biannual basis. Officers may be required to confirm they have read documentation and have understood the intervening times.

Only formally trained Authorised Officers will be permitted to authorised applications.

Oversight

Members

The use of RIPA powers will be a standing item on the agenda for the Audit Committee. An annual report will be produced detailing the usage along with any inspections, changes to policy and procedure.

Senior Management

An annual report will be produced detailing the usage along with any inspections, changes to policy and procedure.

The Investigatory Powers Commissioner's Office

The Investigatory Powers Commissioner will keep under review, the exercise and performance by the persons on who are conferred or imposed, the powers and duties under RIPA. This includes those Authorising Officers authorising Covert Directed Surveillance and the use of Covert Human Intelligence Sources and the maintenance of the Central Register.

A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Complaints can be made by persons aggrieved by conduct e.g. direct surveillance. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. The Council is however, under a duty to disclose or provide to the tribunal all documents they require if:

- A Council officer has granted any authorisation under RIPA.
- Council employees have engaged in any conduct as a result of such authorisation.

A disclosure notice requirement is given.

Relevant case law

There is relevant caselaw which includes but is not limited to:

R v Johnson

In this case the Court of Appeal provided criteria that must be adopted if premises used for observation purposes by the Police are not to be disclosed in open court.

Should PCC wish not to disclose the premises used for the observation, then following the rational in this case it would appear that the Authorising Officer must be able to testify that immediately prior to trial:

- he/she visited premises to be used for observation
- he/she obtained and recorded the views of the owner and/or occupier in respect of the use made of the premises and the possible consequences of disclosure which could lead to identification of the premises and occupiers.

Such views must be recorded and the record marked as sensitive. If this issue arises please contact the Director of Governance for appropriate advice.

R v Sutherland 2002

The recording and handling of confidential material (legal privilege) obtained as a result of recording equipment deployed in the exercise area of two police stations. In this matter, the activity exceeded that which had been authorised and the case against Sutherland collapsed. This emphasises the requirement to ensure that all activity is authorised prior to the operation and any errors are reported.

Peck v United Kingdom [2003]

The applicant was filmed by a CCTV camera operated by Brentwood Borough Council in a public street shortly after he had attempted to commit suicide. The council subsequently released two still photographs taken from the CCTV footage to show the benefits of CCTV. Peck's face was not specifically masked. These pictures subsequently appeared on regional television but his face was masked. Peck sought to challenge the authority's decision but was rejected by the Court of Appeal. He took the matter to the European Court of Human Rights where he was successful. The case establishes the right to privacy in a public area, even if it is a reduced level.

Martin v. United Kingdom [2004] European Court App

Alleged disorderly behaviour by M towards neighbour. Local Authority mounted covert surveillance of M on the basis that the surveillance by video was justified as the surveillance was targeted at behaviour which was visible to a neighbour or passer by. Claim of Article 8 infringement settled by agreement with damages awarded to Martin.

R v. Button and Tannahill 2005

Audio and video recording of defendants while in police custody. Audio recording had been RIPA authorised; video recording was not authorised. Video record admitted in evidence although common ground that it had been unauthorised and so obtained unlawfully (in breach of s.6 Human Rights Act 1998). *It was a*rgued on appeal that the trial Court was itself in breach of s.6 by admitting the evidence. Held that the breach of article 8 related to the intrusion upon private life involved in the covert surveillance. So far as a trial Court is concerned: any such breach of article 8 is subsumed by the article 6 (and P.A.C.E.) duty to ensure a fair trial. The trial judge had not acted unlawfully by admitting the evidence.

C v The Police and the Secretary of State for the Home Department (2006, No: IPT/03/32/H)

A former police sergeant (C), having retired in 2001, made a claim for a back injury he sustained after tripping on a carpet in a police station. He was awarded damages and an

enhanced pension due to the injuries. In 2002, the police instructed a firm of private detectives to observe C to see if he was doing anything that was inconsistent with his claimed injuries. Video footage showed him mowing the lawn. C sued the police claiming that they had carried out Directed Surveillance under RIPA without an authorisation. The Tribunal ruled that this was not the type of surveillance that RIPA was enacted to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

"The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers.

APPENDIX 1 Confidential Material

Confidential Material

"Confidential Material" consists of:

- matters subject to legal privilege;
- confidential personal information; or
- 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 his/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, relating;

- to his/her physical or mental health; or
- 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:
- 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 secrecy contained in existing or future legislation.

”Confidential Journalistic Material” includes material acquired or created for the purpose 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.

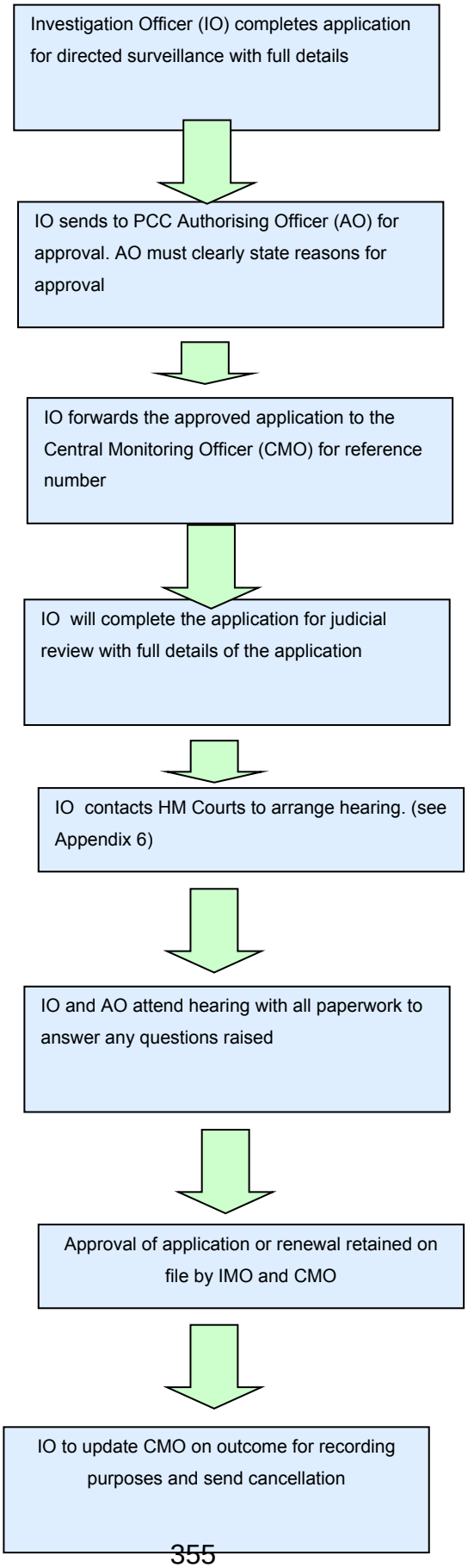
N**ote A.** Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected 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.

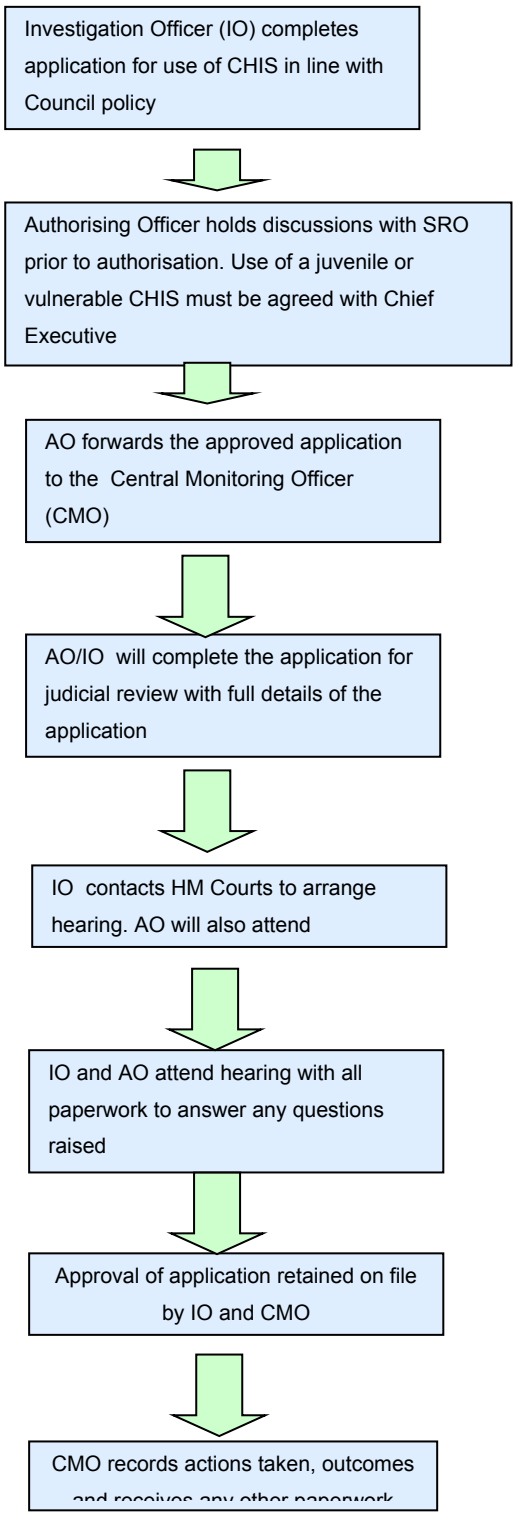
APPENDIX 2 Authorising Officers (RIPA)

Fiona McMillan	Interim Director of Law & Governance	452361	fiona.mcmillan@peterborough.gov.uk
Peter Gell	Head of Regulatory Services	453419	peter.gell@peterborough.gov.uk
Rob Hill	Assistant Director, Communities & Safety	864715	rob.hill@peterborough.gov.uk
Ben Stevenson	Central Monitoring Officer	452387	Ben.stevenson@peterborough.gov.uk

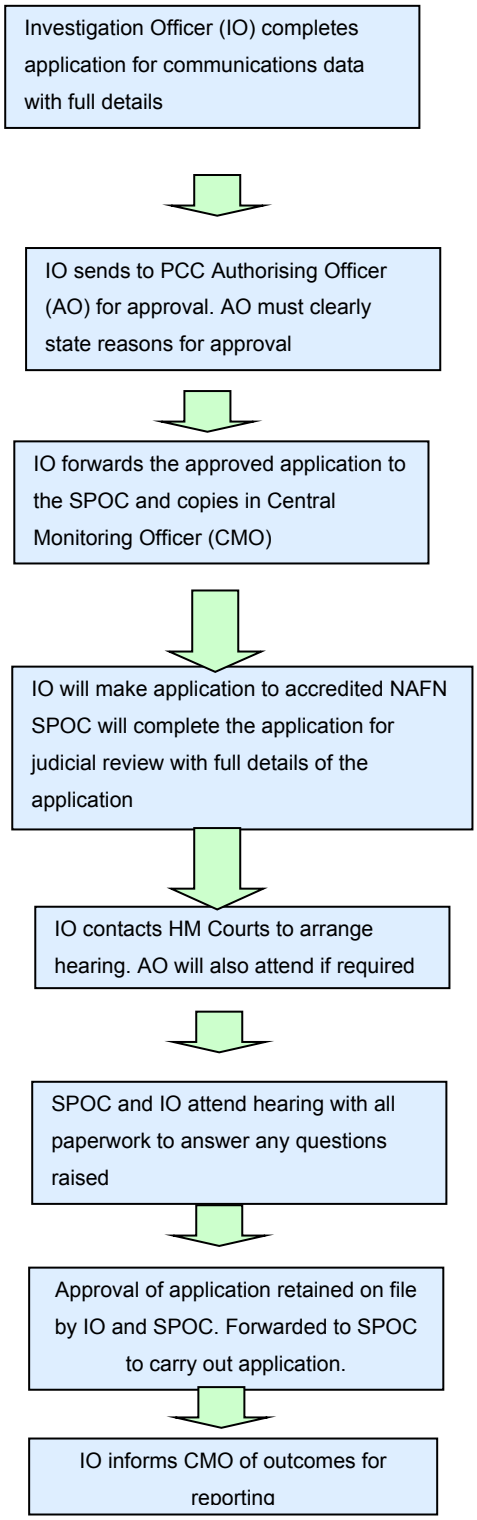
APPENDIX 3 Procedure for directed surveillance application



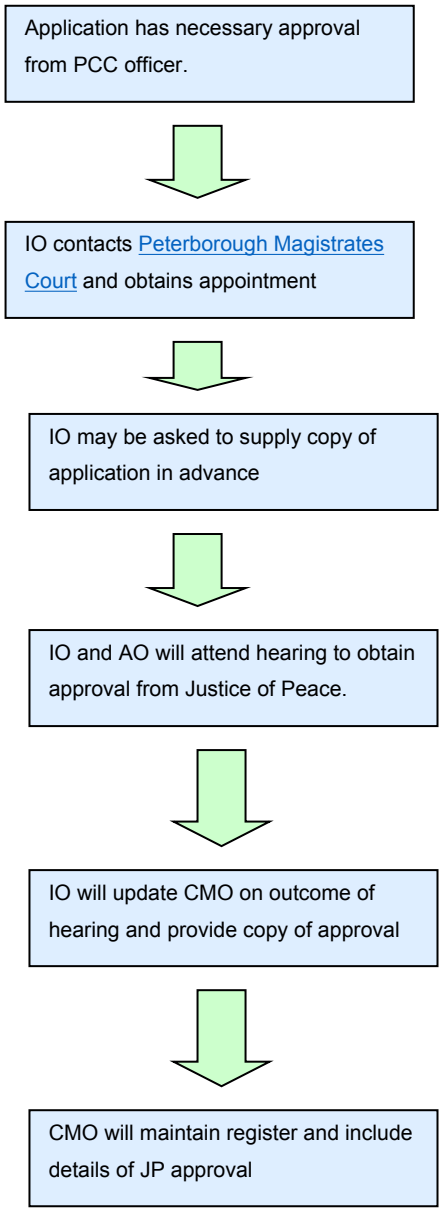
APPENDIX 4 Procedure use of Covert Human Intelligence Source



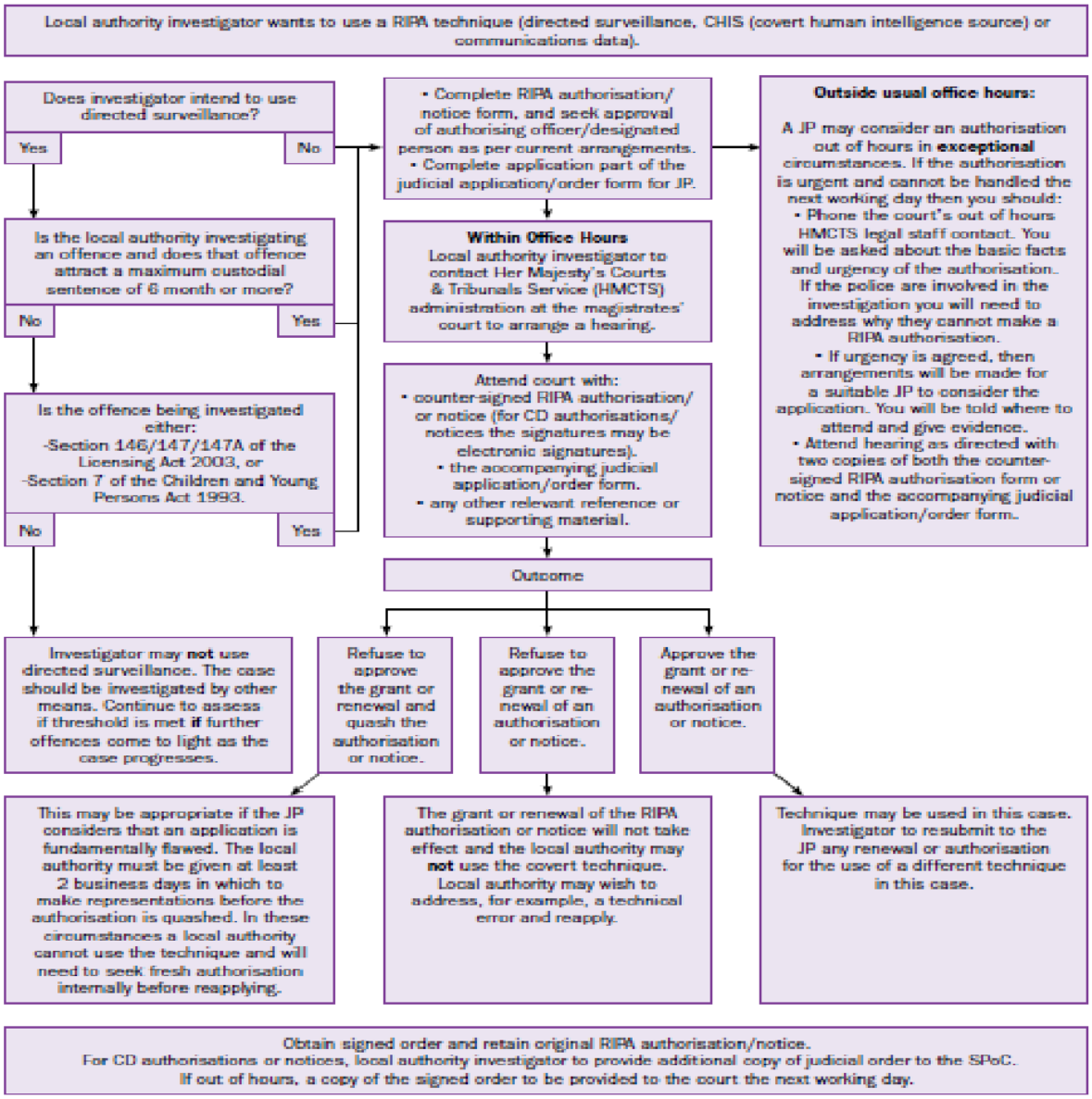
APPENDIX 5 Procedure for obtaining communications data



APPENDIX 6 Procedure for obtaining judicial approval



APPENDIX 7 Statutory process for obtaining judicial approval



APPENDIX 8 Surveillance Assessment

	Notes
Specific location • Type of property • Residents • Number and locations of entrances/exits • Vehicular access • Any obstructions • Any risks	
General Area • Type of area e.g. residential or commercial • Shops in locality • Schools • Any potential hazards	
Subject • Identity • Potentially violent • Vehicles used • Any known other sites	
Collateral intrusion • Detail any other individuals of whom private information may be captured • Associates • Family Children	

● How will it be limited e.g. times, techniques		
<u>Observation Point</u> ● Is location approved? ● Does it require use of another building? ● Routes to and from ● In event of discovery of operation, agreed movement		
<u>Equipment</u> ● What is being used? ● Do they work? ● Any issues regarding signal reception on phones		
Health and Safety Assessment		
Hazard (including who may be harmed)	Level of Risk	Mitigating controls

Appendix 9 – Non RIPA Applications

RIPA Determination Checklist

Name of Applicant		**Team**	
Service			
Directorate			
Line Manager			
I have considered the following and confirm that no activity requiring authorisation under RIPA is required. **If the answer is yes to each question then RIPA did or does apply.**			
Is or was activity considered to be covert surveillance?	Yes	No	
Is or was the surveillance directed?	Yes	No	
Is or was the investigation into a criminal offence?	Yes	No	
Is or was confidential or private information likely to be obtained?	Yes	No	
Did or does the offence meet the crime threshold?	Yes	No	
Signed			
Line Manager/File Review: I have reviewed and considered that there has been no activity which required authorisation under RIPA.			
Name:			
Signed:			
Date:			

Appendix 10 - Social Media/Internet Access Log

Name of Applicant		**Team**	
Service			
Directorate			
Line Manager			
Case including reference			

Visits number	Date	Site Accessed	Reason	Information obtained	Public or Private?

Please note repeated visits will be considered monitoring and you should seek advice on making an appropriate application

You should not use a false identity or build/maintain a relationship to obtain private information about someone.

If you have obtained private information then you should consider an appropriate application

This page is intentionally left blank