Peterborough City Council

Cambridgeshire County 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 and Cambridgeshire County 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, Peterborough City Council
Other documents that link to this one:	RIPA toolkit on Insite and CamWeb
Document ratified/approved by:	Audit Committee, Peterborough City Council Audit Committee, Cambridgeshire County Council
Version number:	Version 1.5
Issue date:	August 2021
Dissemination method:	Notification to staff via the Weekly Round-up newsletter and via All Staff notifications on the front page of Insite. Notification to staff via CamWeb
Date due for review:	August 2022
Reviewer:	Director of Law 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
Review in light of code of practice changes and inspection comments	4	March 2019
Review in light of code of practice changes and inspection comments	5	August 2021

2

Contents

3

4

5

1. 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 Councils' 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

1.1 Key Role Definitions

Senior Responsible Officer – the Senior Responsible Officer (SRO) provides senior management oversight of the use of RIPA and provides assurance and integrity for the process. This will include oversight of authorisations, errors, reporting, training and inspection.

The SRO for both Peterborough City Council and Cambridgeshire County Council is Fiona McMillan, Director of Law & 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.

The CMO for both Peterborough City Council and Cambridgeshire County Council 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.

1.1 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

2. 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 for more detail.

9

3. General Observation Activities

The general observation duties of council officers will not require authorisation under RIPA whether covert or obvert. Such duties form part of the functions we are required to provide as opposed to pre-planned surveillance of a person or group. Paragraph 3.33 of the Revised Code of Practice provides some examples of when an authorisation may not be required.

Example: Plain clothes police officers on patrol to monitor a high street crime hot-spot or prevent and detect shoplifting would not require a directed surveillance authorisation. Their objective is merely to observe a location and, through reactive policing, to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. **A directed surveillance authorisation need not be sought.**

Example: Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again, this is part of the general duties of public authorities and the obtaining of private information is unlikely. **A directed surveillance authorisation need not be sought**.

Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine her suspected involvement in shoplifting. It is proposed to conduct covert surveillance of Z and record her activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy, and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. **A directed surveillance authorisation should therefore be considered.**

4. Covert Surveillance

4.1 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.

4.2 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.

4.3 When is surveillance directed?

Surveillance is 'Directed' (paragraph 2.2 of the Revised Codes of Practice) 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.

4.4 When is Surveillance Intrusive?

LOCAL AUTHORITIES ARE NOT AUTHORISED TO

CARRY OUT INTRUSIVE SURVEILLANCE

Surveillance is intrusive, (paragraph 3.19 of Revised Codes of Practice) if it is covert and:

- is carried out in relation to anything taking place on any "residential premises" or
- in any "private vehicle" (see below); and
- involves the presence of an individual or surveillance device in the premises or in the vehicle, or
- is carried out by a means of a surveillance device

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.

A private vehicle is defined in the Act as any vehicle which is primarily used for the private purposes of the person who owns or has the right to use it. This would include company cars and leased cars used for business and pleasure. This is distinct to vehicles owned or leased by public authorities. Paragraph 7.49 of the Revised Codes of Practice provides guidance on

11

the latter; if devices are used within a council owned vehicle with the knowledge of the occupants, then this is not considered to be surveillance however hidden devices may require authorisation.

5. Authorising 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 considered):

(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 and
(c) fair and balanced

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.

12

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.

The application should also be presented in a fair and balanced way which should include evidence or information which weakens the case for authorisation.

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 have also undertaken a surveillance assessment which includes a health and safety risk assessment, Appendix 7.

Judicial approval should then be sought. The corporate procedure for this can be found in Appendix 5.

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

6. The Surveillance Checklist for Applicants

Before a council officer 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.

6.1 Is the Surveillance Necessary?

Any application granted must consider that the activity is necessary on one or more of the statutory grounds. In the case of the council then this will be for the prevention and detection of crime in line with the crime thresholds described below.

6.2 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.

6.3 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 when applying for the appropriate authority.

6.4 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.

Paragraph 3.3 of the Revised Code of Practice provides scope for what information which may not be is not private may include publicly available information such as books, newspapers, TV and radio broadcasts, business reports and websites.

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

6.5 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 6 months or more 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.

6.6 Is it proportionate?

In determining whether the activity is proportionate, paragraph 4.7 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?

7. 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.

8. CCTV

Peterborough City Council operates a CCTV system which can be used in surveillance where appropriate and where authorised. The CCTV system is overt and is governed by the Surveillance Camera Code of Practice and the ICO guidance on the matter. This does not mean that the use of overt cameras for surveillance does not require authorisation under the Act. It may be considered covert, pre-planned and directed towards a person or group which would require authorisation.

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.

8.1 Use of CCTV system by Cambridgeshire Police

Where the CCTV systems is being operated by Police officers under a RIPA authorisation, we will maintain a register of the details of the date and time of the authority was granted, the nature of the offence under investigation and the operation name an*d/*or authority reference number.

If council officers operate the CCTV under direction of the police, the council will be provided with a redacted authorisation which shows the details of the date and time of the authority being granted, the activity authorised and its boundaries and limitations, the nature of the offence under investigation, the operation name and*/*or authority reference number.

8.2 Cambridgeshire County Council CCTV

Cambridgeshire County Council have and have access to a number of cameras which are primarily for bus lane enforcement, highways and libraries. These are governed by the codes as described above. These cameras are primarily used for reactive footage but were they to be considered for any directed surveillance then the process used for Peterborough City Council would be followed.

8.3 Aerial covert surveillance

Whilst the councils do not currently utilise aerial surveillance devices such as drones or helicopters, any use in the future or by contracted providers should be considered for authorisations.

9. Covert Use of Human Intelligence Source ("CHIS")

Before use of a CHIS is authorised, advice must be sought from the Senior Responsible Officer or their appointed deputy. The application can be authorised by the Chief Executive (or an appointed deputy) and the applicant must ensure that they as Authorising Officer have sufficient information to make an informed decision the prescribed forms must be fully completed.

9.1 What is a CHIS?

The Revised Codes of Practice for Covert Human Intelligence Source (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.

9.2 When a CHIS and when not a CHIS?

The following give examples of when a CHIS would and would not be needed.

Would not need a CHIS authorisation	Would need a CHIS authorisation
Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited regarding the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should	In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence, the public authority decides to deploy its operative on several occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

be given to granting a directed surveillance authorisation.	
A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.	A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.
A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual	Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not 14 established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague

9.3 Conditions for authorisation of Covert Human Intelligence Sources

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 benefit fraud hotline).

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

19

9.3.1 Necessity and Proportionality

The necessity and proportionality principles apply but the crime threshold does not apply in this area.

If the authorising officer considers it to be necessary, then they should consider proportionality as below:

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation; •
- evidence, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought.

9.3.2 The Authorised Conduct

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.

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 maximum time limit for authorisation is 12 months for an adult CHIS.

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

9.3.3 Operational Considerations

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 20

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 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 accurate and proper information supplied by the CHIS
- Monitoring the CHIS's security and welfare

A senior manager, not the Authorising Officer, will always 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.

9.4 Operation involving multiple CHIS

A single authorisation may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several individual operatives acting as a CHIS in situations where the activities to be authorised, the subjects of the operation, the interference with private or family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each officer. If an authorisation includes more than one relevant source, each relevant source must be clearly identifiable within the documentation. In these circumstances, adequate records must be kept of the length of deployment of a relevant source to ensure the enhanced authorisation process set out in the 2013 Relevant Sources Order and Annex B of the Code of Practice can be adhered to.

9.5 Use of a Juvenile as a CHIS or in Directed Surveillance

Paragraph 4.2 of the CHIS Code of Practice refers to the use of juveniles in either scenario and how special safeguards also apply to the use or conduct of juveniles. The use of such a person could occur during test purchasing operations. The Code of Practice gives clear guidance:

21

- On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them.
- In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.
- Authorisations for use of a juvenile as a CHIS should be granted by the Head of Paid Service i.e., the Chief Executive.
- The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review.
- For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

We must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g., someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). Any deployment of a juvenile CHIS should be subject to the enhanced risk assessment process set out in the statutory instrument, and the rationale recorded in writing.

The below give examples of when the juvenile may be a CHIS and when a directed surveillance application may be more appropriate.

CHIS authorisation not needed	CHIS authorisation needed
Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited regarding the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS,	In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence, the public authority decides to deploy its operative on several occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

consideration should be given to granting a directed surveillance authorisation.	

9.6 Security and welfare

When considering deploying a CHIS, the council should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that deployment/tasking.

Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any deployment and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained.

The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS.

Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example, this could be by means of disclosure to a court or tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 8.22 to 8.25 of the CHIS Code of Practice.

The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether to allow the authorisation to continue.

9.7 Considering a Covert Human Intelligence Source (CHIS) authorisation in social media/internet investigations

Any council officer or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether via publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation.

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

9.7.1 Tasking someone to use a profile for covert reasons

Where someone, such as an employee or member of the public, is tasked by the council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

Example of when CHIS authorisation is needed
• An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person. • Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose. • Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

9.7.2 Registering to access a site

A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where an officer sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example of when CHIS authorisation is not needed	Example of when CHIS authorisation is needed
A Trading Standards officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that counterfeit goods are being	A Trading Standards officer tasks a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller,

sold. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed, and a CHIS authorisation need not be sought.	country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

9.7.3 Use of Likes and Follows

Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not, in itself, constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for a council officer or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example of when CHIS authorisation is not needed	Example of when CHIS authorisation is needed
An officer maintains a false persona, unconnected to law enforcement activities, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity, they “follow” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed, and no CHIS authorisation is needed.	The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.

9.7.4 The identity being used

When engaging in conduct as a CHIS, a council officer 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 considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

9.7.5 Risk Assessment

Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 of the CHIS Code of Practice should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of

any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved.

10. Use of social media/internet in investigations

The use of the internet and social media sites such as Facebook, Instagram and Twitter in an investigation is permitted and may be a means of gathering intelligence. In accessing such sites, officers must consider the issues of privacy and collateral intrusion. The Revised Code of Practice sections 3.10 to 3.17 provides good guidance on the subject.

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.

Where information about an individual is placed on a publicly accessible database such as Companies House, then they are unlikely to have expectations of privacy.

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 investigation.

The following from the Code of Practice is a guide of factors to consider

- Whether the investigation or research is directed towards an individual or organisation
- Whether it is likely to result in obtaining private information about a person or group of people
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile

26

- Whether the information obtained will be recorded and retained
- Whether the information is likely to provide an observer with a pattern of lifestyle
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s)
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties

Any similar activity carried out on the council's behalf by a third party then this may still require a directed surveillance authorisation.

10.1 "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.

10.2 Using a covert accounts and identities

Where officers are building and maintaining a relationship with an individual without that individual knowing the true nature for the purposes of an investigation, this may require an application for the use of a CHIS. Guidance is provided in section

If officers create a false or covert identity, this must only be created with the approval of an Authorising Officer and the CMO must be informed. All use of the identity must be logged and reported to the CMO.

Any use of the internet in an investigation must be fully documented, Appendix 10 may be used as a template.

10.3 Council policy on reviewing use of social media during investigation

Misuse of council devices or misuse of social media may be considered in line with the relevant disciplinary policy. Any usage should be considered in line with the council's social media policy and this policy.

Both councils have the capability to "audit" the use of social media sites by individual user's profile in line with the appropriate IT policies. The council will undertake such an audit in the event of a complaint or concern that social media has been misused or accessed during an investigation where RIPA may apply and has not been appropriately applied for. The concern will be raised with the Central Monitoring Officer and Data Protection Officer who will advise on the appropriate procedure.

The council may also undertake spot check audits where investigators or staff will be required to detail the reason for access.

11. Surveillance 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 includes 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.

29

11.1 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 4.31 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 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.

It may be necessary for the councils to work with a third party who are not considered a public authority by the Act. In those cases, the third party are acting as an agent for the council and therefore an authorisation should be considered by the councils.

11.2 Combined Authorisations

In line with Codes of Practice paragraph 4.17, 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.

11.3 Lapse of Authorisations

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

Covert Human Intelligence Source - 12 months from the date of the approval of a magistrate (or last renewal) for adult or 4 months for a juvenile.

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

11.4 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. Prior to this, the Authorising Officer should ensure a review has been carried out using the same criteria as if it were a new application.

For the conduct of a Covert Human Intelligence Source, this should not be renewed 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 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.

11.5 Retention Period for Authorisations

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

11.6 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.

11.7 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 applicant must also undertake a review throughout the matter and inform the Authorising Officer if the authorisation is no longer required.

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.

11.8 Immediate response to situations

The ability for a local authority to grant urgent oral authorisation for use of RIPA is not permitted. 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.

12. Data Protection & Data Assurance

All material obtained by the councils during authorised activities such as photographs, videos, and notes should be protected against loss and alteration. The councils have data protection policies and ICT security policies to ensure that the councils are compliant with the handling of such information.

Authorising officers must ensure compliance with the appropriate data protection requirement such as a data protection impact assessment if necessary as well as the relevant codes of practice in the handling and storage of material.

Information, materials and evidence collected during an investigation

Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the UK General Data Protection Regulation, Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the councils' policies and procedures currently in force relating to document retention. These are available on both councils' intranets in the Information Governance sections.

The following paragraphs give guidance on some specific situations, but advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer where appropriate.

- Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with legal disclosure requirements. All such material should be clearly labelled and stored in such a way to enable compliance with data retention and disposal.
- Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether 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 councils of any material obtained by means of covert surveillance, unless directed by court order, and other than in pursuance of the grounds on which it was obtained requires authorisation by the Senior Responsible Officer.

12.1 Sharing information

Material obtained should only be shared with individuals within the authority and external partners where this is permitted by legislation, an information sharing agreement or a requirement to disclose. For example, a joint investigation with the Police would require information to be shared as part of that investigation and permitted by data protection legislation.

12.2 Publishing CCTV footage to enable suspect identification

Any consideration of publishing images or film of those believed to have committed an offence or have involvement in an offence must consider the rights and privacy of anyone in those images or film. Failure to do so may result in a breach of data protection legislation and lead to regulatory action. The Senior Responsible Officer and Data Protection Officer must be consulted ahead of any decision.

12.3 Storage

Any material obtained must be stored securely, either electronically or physically, and access only provided to those who have the appropriate clearance for access. Physical information must be protected by an adequate level of security such as locked rooms or a safe with a log of access kept.

12.4 Destruction

Information will be destroyed securely in line with retention requirements and its retention will be reviewed accordingly.

13. Other Factors

13.1 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.

13.2 Confidential or Privileged Material

Consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes:

- where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. (9.29 to 9.35)
- confidential journalistic material or where material identifies a journalist's source, (9.36 to 9.46)
- where the material contains information that is legally privileged, (9.47 to 9.75)

Guidance on each of these can be found in the Revised Codes of Practice as noted above. In the event that these types of information may be acquired, officers should consult the Revised Codes of Practice and the SRO.

Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material may be authorised only by the Chief Executive (or a deputy in their absence. 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 Director of Law and 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 Director of Law and Governance) 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.

13.3 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.

13.4 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.

13.5 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.

14. 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 CMO 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.

15. 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”.

16. 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”.

17. 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 following 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.

There is no threshold for subscriber data which can still be acquired for any crime where it is necessary and proportionate to do so. However as of 1 November 2018, there is a crime threshold for the acquisition of service or traffic data which is restricted to "serious crime". This is defined as:

- An offence capable of attracting a prison sentence of 12 months or more. This can be checked by accessing the Home Office counting rules notifiable offence list.
- An offence by a person who is not an individual i.e., a corporate body
- A Section 81 of RIPA – an offence defined as serious crime such as use of violence, substantial financial gain or large number of people in pursuit of a common purpose
- An offence which integrally involves the sending of a communication
- Breach of privacy offence

Examples of what are non-serious crimes are:

- Certain immigration offences under the Immigration Act 1971; and

- Certain gambling offences under the Gambling Act 2005 including provision of facilities for gambling, use of premises for gambling and offences relating to gambling machines.
- Some sections of the Public Order Act which do not amount to violence (including using offensive words or causing a fear of violence);
- Driving offences, such as: joy riding, driving when disqualified, failure to stop or report an accident and driving when unfit to do so through drink or drugs;
- Some sections of the Consumer Protection Act 1987 i.e. furnishing false information in response to notice, or to enforcement officer.

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.

17.1 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 purpose of the application in terms of the prevention or detection of crime (section 22(2) (b) of the Act)
- 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.
- A description of the offence and how this meets the serious crime threshold if it is for traffic or service data
- 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.

18. 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.

19. Oversight

19.1 Members

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

19.2 Senior Management

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

20. 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 Councils are 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.

39

- council employees have engaged in any conduct as a result of such authorisation.

A disclosure notice requirement is given.

21. 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 passerby. 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.

41

AB v Hampshire Constabulary (Investigatory Powers Tribunal ruling 5 February 2019)

This case relates to whether the use of body worn cameras can amount to surveillance as defined by legislation. In this matter, the Tribunal concluded that in this case video recording was capable of amounting to surveillance under Part II of RIPA (2000). The decision can be viewed here. https://www.ipt-uk.com/docs/IPT%20Judgment%20-%20AB%20v%20Hants%20Constabulary.pdf

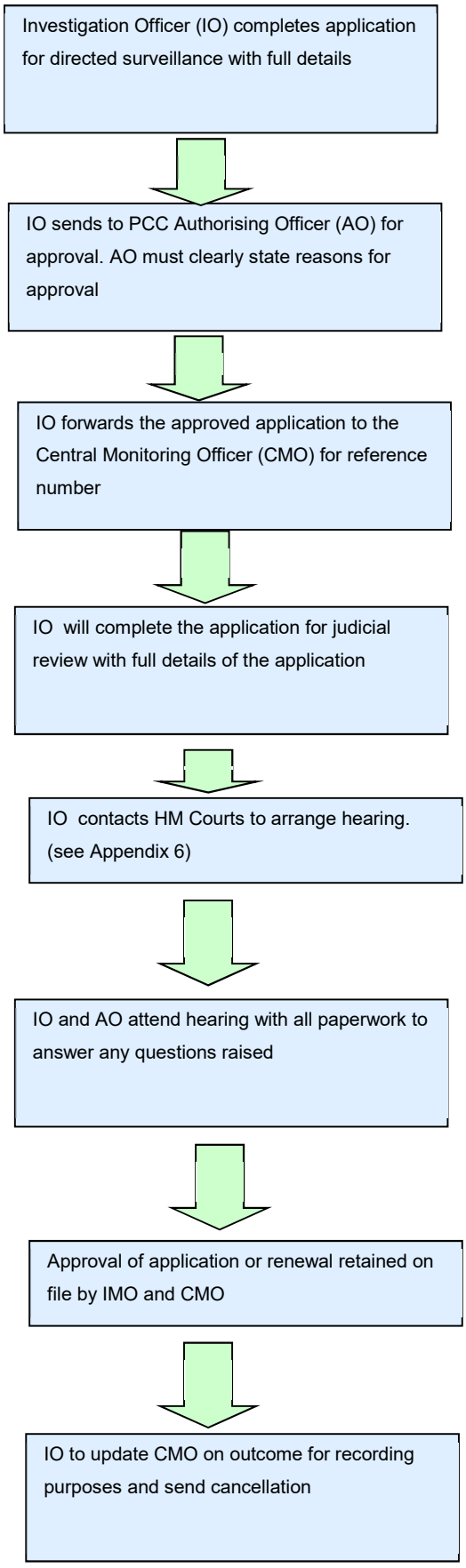
Gary Davies v British Transport Police (Investigatory Powers Tribunal 5 February 2019

British Transport Police undertook unauthorised surveillance which led to a public arrest and a press release publicising the alleged offences. Mr Davies was subsequently acquitted by a jury. British Transport Police officers had no proper understanding of the legal requirements for such surveillance and should have obtained authorisation. The surveillance was ruled unlawful. The Tribunal rejected the British Transport Police claim that the breach was technical as authorisation could and would have been obtained. This was rejected because the case against Mr Davies required further inquiries to have been made for authorisation to be possible. The Tribunal awarded Mr Davies costs of the criminal trial and also £25,000 in compensation for damages to his reputation suffered and harm caused.

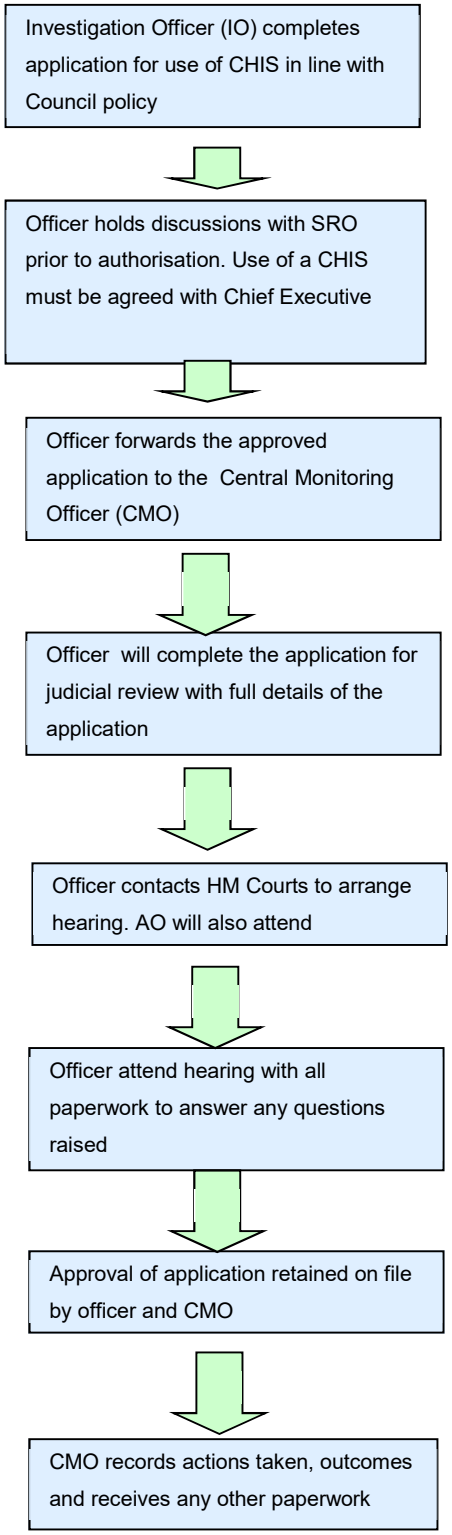
APPENDIX 1 Officers (RIPA)

Senior Responsible Officer			
Fiona McMillan	Director of Law & Governance, PCC & CCC	01733 452361	fiona.mcmillan@peterborough.gov.uk fiona.mcmillan@cambridgeshire.gov.uk
Authorising Officers			
Peter Gell	Assistant Director, Regulatory Services PCC & CCC	01733 453419	peter.gell@peterborough.gov.uk
Rob Hill	Assistant Director, Communities & Safety PCC & CCC	01733 864715	rob.hill@peterborough.gov.uk
Central Monitoring Officer for PCC and CCC			
Ben Stevenson	PCC	01733 452387	Ben.stevenson@peterborough.gov.uk

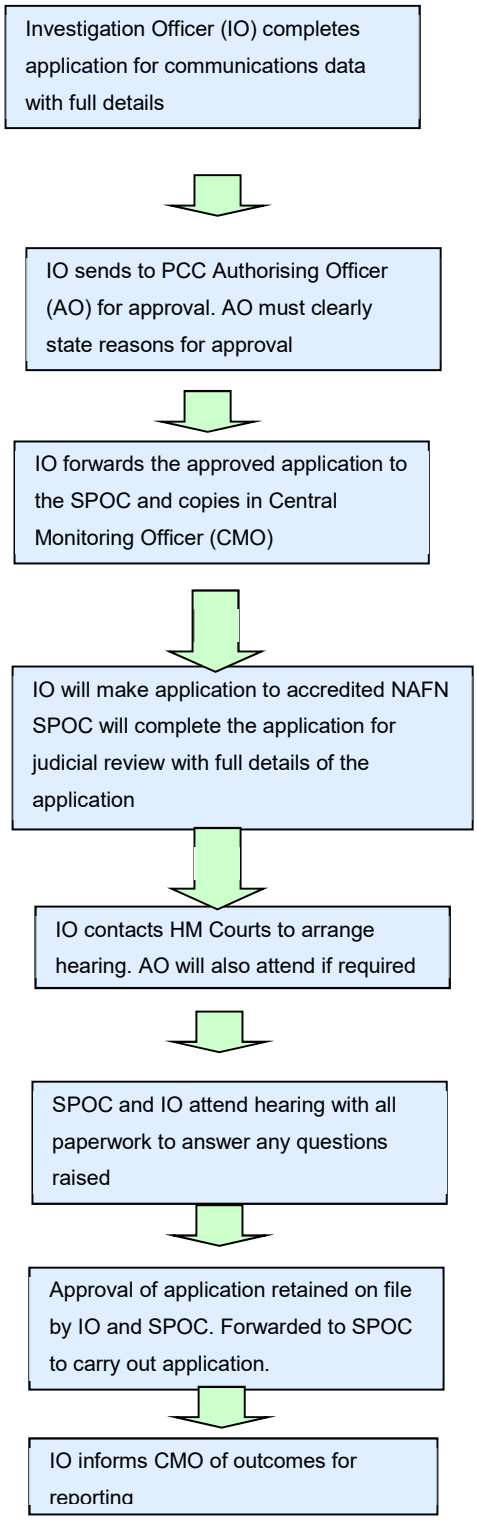
APPENDIX 2 Procedure for directed surveillance application



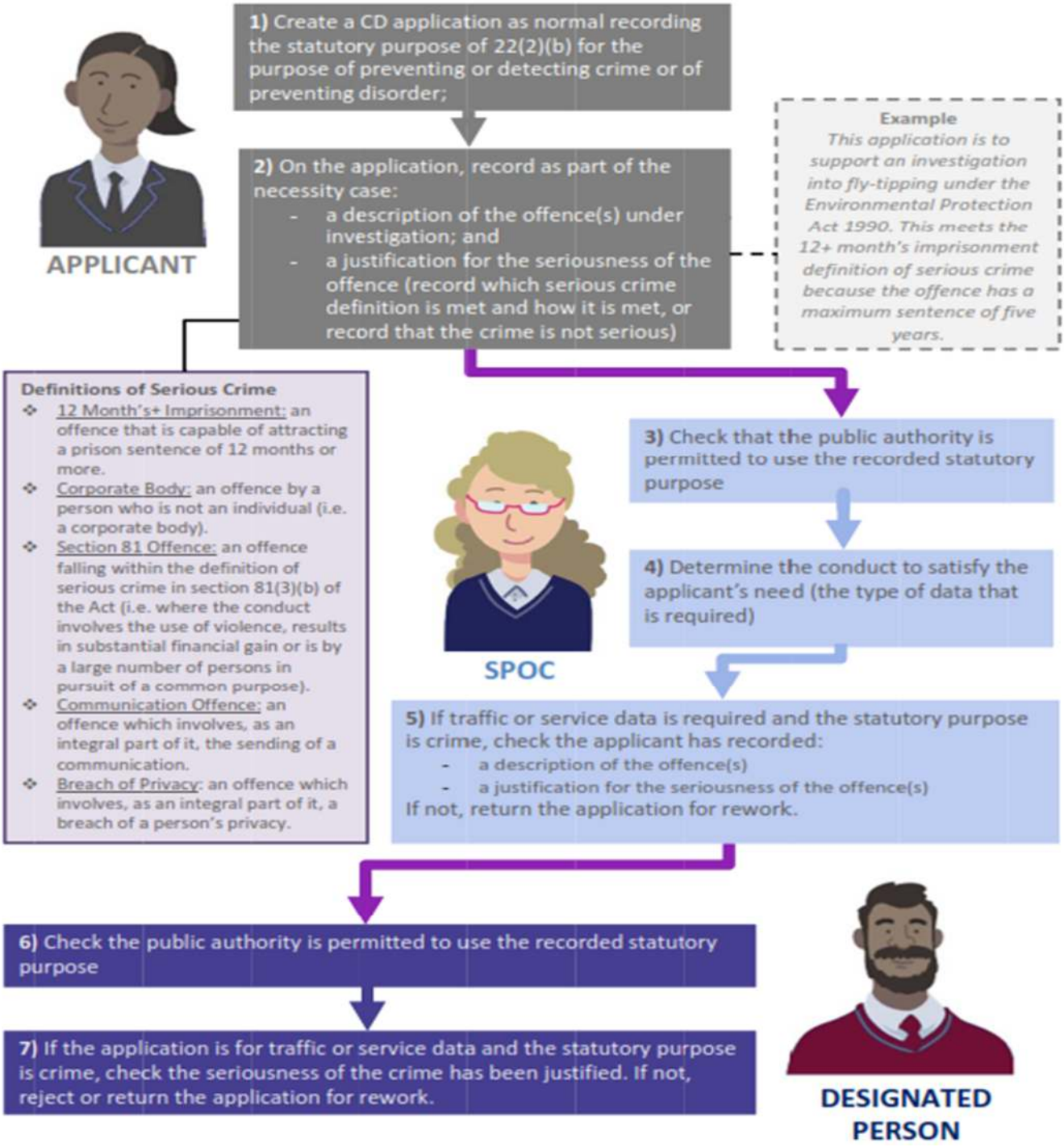
APPENDIX 3 Procedure use of Covert Human Intelligence Source



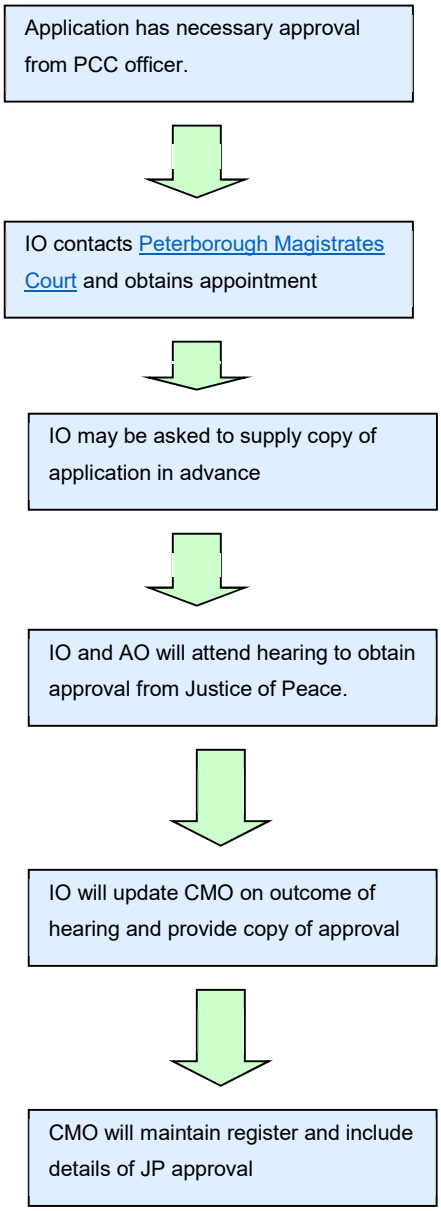
APPENDIX 4 Procedure for obtaining communications data



APPENDIX 5 Flow Chart of Changes to Communications Data (November 2018 onwards)



APPENDIX 6 Procedure for obtaining judicial approval



APPENDIX 7 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	
Observation Point ● Is location approved? ● Does it require use of another building? ● Routes to and from ● In event of discovery of operation, agreed movement	
Equipment	

● 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

50

APPENDIX 8 – 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:			

51

Date:

52

APPENDIX 9 - 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