

Report of:	Meeting	Date	Item no.
Mary Grimshaw, Legal Services Manager	Audit Committee	19 November 2019	

Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)

1. Purpose of report

- 1.1 To review the authority's use of RIPA since it was last considered at the Audit Committee in September 2017.
- 1.2 To note the outcome of the 'RIPA' desktop inspection by the Investigatory Powers Commissioner's Office (IPCO).
- 1.3 To approve the proposed changes to the council's 'RIPA' policy as detailed in this report.

2. Outcomes

- 2.1 Evidence that the Council complies with current legislation.

3. Recommendations

- 3.1 Members are requested to note that there have been no authorisations granted for directed surveillance or covert human intelligence source under the Regulation of Investigatory Powers Act 2000 since 2012.
- 3.2 Members are requested to approve the revised RIPA policy attached at Appendix A to reflect the guidance contained in the revised Code of Practice for Covert Surveillance and Property Interference (August 2018).

4. Background

- 4.1 Local authorities can undertake surveillance and access communications data under the framework of the Regulation of Investigatory Powers Act 2000. These rules set high standards for all public authorities that use these powers to undertake a range of enforcement functions to ensure

they can keep the public safe and bring criminals to justice, whilst protecting individuals' rights to privacy.

- 4.2** From 1 November 2012, the Protection of Freedoms Act 2012, became effective. It introduced a more restrictive approach to the use of RIPA by local authorities by limiting the use of direct authorisations to serious crimes, i.e. those crimes punishable by a maximum custodial sentence of six months or more or those constituting an offence of selling alcohol or tobacco to children. The application must also have judicial approval by a magistrate before an authorisation takes effect and the magistrate needs to be satisfied that there are reasonable grounds for believing that the requirements of RIPA are met.

5. Key Issues and proposals

- 5.1** The Home Office Code of Practice requires a number of best working practices to be adopted by all public authorities, including:

- An annual review of the authority's use of RIPA to ensure that it is being used consistently and in accordance with the Council's policy; and
- An annual review of the policy ensuring that it remains fit for purpose.

- 5.2** As the council's three yearly RIPA inspection was due in autumn/ winter 2018, it was decided to defer the annual review in 2018 until after the inspection had taken place.

- 5.3** There is a requirement for the Council to nominate a Senior Responsible Officer, who will be responsible for:

- The integrity of the RIPA process in place within the Council to authorise surveillance and the covert use of human intelligence source (CHIS);
- Compliance with the legislation and codes of practice;
- Engagement with the Commissioners and inspectors when they conduct their inspections; and
- Overseeing the implementation of any post inspection action plan recommended by the Commissioner.

- 5.4** There is also a requirement to have a Senior Responsible Officer who oversees the competence of Authorising Officers and the processes in use in the authority. Both of these roles are allocated to the Legal Services Manager.

- 5.5** There has been no authorisations issued under RIPA since 2012.

- 5.6** The Investigatory Powers Commissioner's Office (IPCO) has recently taken over the inspection and oversight functions on RIPA, previously carried out by the Surveillance Commissioner's Office and the inspection which was due in autumn/winter 2018, did not take place until March 2019.
- 5.7** The IPCO and his assistants have confirmed that they will continue to ensure RIPA compliance by conducting a programme of inspections of Local Authorities. As a generality, they aim to inspect each council in England, Wales and Scotland once every three years but have introduced remote desktop inspections when a local authority has significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns. However, a desktop inspection will always be followed by an onsite inspection.
- 5.8** The Council's most recent inspection was carried out by a remote assessment in March 2019.
- 5.9** Following the desktop-based documentary inspection, the Inspector issued a report in April 2019, which concluded that the Council's policy and guidance regime was clear and comprehensive and that regular refresher training carried out by the officers was appropriate. He drew the council's attention to the usefulness and accessibility of social media in assisting with the council's enforcement processes and the advice contained in the revised Home Office Covert Surveillance and Property Interference Code of Practice. A copy of his report is attached at Appendix B.
- 5.10** In light of the Inspector's report and following refresher training undertaken by officers where the use of social media was addressed, paragraph 11 of the Council's policy at Appendix A has been updated, together with a few other minor changes. The amendments are highlighted for members' attention via the use of 'track changes' A new social media process has also been added at Appendix 11 which outlines the process to be followed by officers when considering using social networking sites for enforcement purposes, in investigations or to gather evidence.

Financial and legal implications	
Finance	There are no direct financial implications associated with the changes. Training for staff, to ensure that they are kept up to date with good enforcement practices and revisions to RIPA, will be met from existing budgets.
Legal	The approval of the recommendation will ensure that the statutory requirements have been complied with.

Other risks/implications: checklist

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report for those issues marked with an X.

risks/implications	✓ / x
community safety	x
equality and diversity	x
sustainability	x
health and safety	x

risks/implications	✓ / x
asset management	x
climate change	x
ICT	x
data protection	✓

Processing Personal Data

In addition to considering data protection along with the other risks/ implications, the report author will need to decide if a 'privacy impact assessment (PIA)' is also required. If the decision(s) recommended in this report will result in the collection and processing of personal data for the first time (i.e. purchase of a new system, a new working arrangement with a 3rd party) a PIA will need to have been completed and signed off by Data Protection Officer before the decision is taken in compliance with the Data Protection Act 2018.

report author	telephone no.	email	date
Mary Grimshaw	01253 887214	Mary.grimshaw@wyre.gov.uk	25.10.2019

List of background papers:		
name of document	date	where available for inspection
None		

List of appendices

Appendix A – Updated RIPA Policy

Appendix B - Inspector's Report



Wyre Borough Council

Policy Statement

The Regulation of Investigatory Powers Act, 2000 (RIPA)

November 2016
(reviewed September 2017)

|

[Reviewed May 2019](#)

Contents

Chapter		Page
1.	Introduction	1
2.	Directed Surveillance	2-4
3.	Covert Use of Human Intelligence Source (CHIS)	4-6
4.	Duration, Authorisation, Reviews, Renewals and Cancellations	7-13
5.	Communications Data	13-14
6.	Other Factors to Consider	15-17
7.	Central Register	17
8.	Codes of Practice	17
9.	Benefits of Obtaining Authorisations under RIPA	18
10.	Scrutiny and Tribunal	18
11.	Covert Surveillance of Social Networking Sites(SNS)	19-20
12.	Conclusion	20
	Appendix 1 - Definitions	21-22
	Appendix 2 - Scheme of Delegation	23-24
	Appendix 3 - Examples	25-26
	Appendix 4 - Codes of Practice (www.homeoffice.gov.uk Covert Surveillance and Property Interference, Covert Human Intelligence)	

Sources and Acquisition & Disclosure of

Communications Data Sources) 2014

Appendix 5 -RIPA 2000

www.homeoffice.gov.uk

Appendix 6 OSC Procedures and Guidance

surveillancecommissioners.independent.gov.uk
<https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf>
www.legislation.gov.uk

Appendix 7 - s.37 and 38 of the Protection of Freedoms Act 2012 and RIPA (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012.

Appendix 8 – Home Office Guidance Protection of Freedoms Act 2012.

www.homeoffice.gov.uk

Appendix 9 – RIPA Forms

intranet - RIPA

Appendix 10- RIPA Directed Surveillance Decision Chart for Local authorities

27

Appendix 11-Process for using Social Networking Sites.

28

1. Introduction

- 1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.
- 1.2 Wyre Borough Council is therefore included within the RIPA framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources and access to Communications Data.
- 1.3 The purpose of this guidance is to:-
- explain the scope of RIPA and the circumstances where it applies
 - provide guidance on the authorisation procedures to be followed.
- 1.4 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and copies are attached at Appendix 4.
- 1.5 In summary, RIPA requires that when the Council undertakes “directed surveillance” ~~or~~ uses a “covert human intelligence source” or “accesses communication data”, these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. Following changes made by the Protection of Freedoms Act 2012 all authorisations must be approved by a magistrate from 1st November 2012. ~~An extract from the Scheme of Delegation indicating the Authorising Officers is attached at Appendix 2.~~
- 1.6 Authorisation under RIPA gives lawful authority to carry out directed surveillance and the use of a covert human intelligence source. Obtaining authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention on Human Rights which is now enshrined in English law through the Human Rights Act 1998. ~~This is because the interference with the private life of citizens will be “in accordance with the law”. Provided activities undertaken are also “reasonable and proportionate” they will not be in contravention of Human Rights legislation.~~
- 1.7 Authorising Officers and investigators within the Local Authority are to note that RIPA does not extend powers to conduct Intrusive Surveillance (see para 2.4.5). ~~Investigators should familiarise themselves with the provisions of the Code of Practice on Directed Surveillance and Covert Human Intelligence Sources (Appendix 4) to ensure a good understanding of the limitation of powers within RIPA.~~

- 1.8 [Deciding when authorisation is required](#) involves making a judgment. Paragraph 2.4 explains this process in detail. If you are in doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Senior [Responsible Officer](#), [Solicitor](#).

2. Directed Surveillance

2.1 What is meant by Surveillance?

“Surveillance” includes:-

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

2.2 When is surveillance directed?

Surveillance is ‘Directed’ for the purposes of RIPA if it is covert, but not intrusive and is undertaken:

- a) for the purposes of a specific investigation or a specific operation.
- b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
- c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

2.3 Surveillance becomes intrusive if the covert surveillance:

- a) is carried out in relation to anything taking place on any **“residential premises”** or in any **“private vehicle”**; and
- b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or
- c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

It should be noted that the Council cannot authorise “intrusive surveillance”.

2.4 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 the following key questions need to be asked.

2.4.1 *Is the surveillance covert?*

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

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

Examples of surveillance are provided in the Code of Practice 2014 and are summarised in Appendix 3.

2.4.2 *Is it for the purpose of a specific investigation or a specific operation?*

If Officers are monitoring general activity in a street or car park, whether covert or overt, then it is not covered by RIPA, as such general observation duties are part of the legislative functions of public authorities and are not pre-planned surveillance of a specific person or group of people.

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

“Private information” is any information relating to a person’s private or family life.

It is an issue of fact and degree, which has to be examined in each case.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person’s activities 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.

Example: Officers of a local authority wish to drive past a café for purpose of taking a photograph of the exterior. This is not likely to require a directed surveillance authorisation, as no private information about any person is likely to be obtained. However if the authority, wish to establish a pattern of occupancy of the premises, the accumulation of information is likely to result in the obtaining of private information and a direct surveillance authorisation should be considered.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside RIPA.

2.4.4 **Otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation**

~~The Home Office Code of Practice 2014 gives An the~~ example of an immediate response to something happening during the course of an observer's work, which is unforeseeable ~~-would bee.g.~~ a housing benefit fraud officer who conceals himself and continues to observe a person working who he knows to be claiming benefits and whom he comes across unexpectedly.

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

2.4.5 **Surveillance - Directed or Intrusive?**

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Commercial premises and commercial vehicles are therefore excluded from intrusive surveillance.

High quality video monitoring or CCTV cameras may run a significant risk of providing consistently high quality data "as if you were there" and therefore come within the definition of intrusive surveillance.

~~Matron~~ boxes ie. noise monitors, used by environmental health departments will not usually be covered. ~~–Usually~~ they are stationed in a neighbouring property and do not provide evidence of the same quality as if the device was actually on the premises. ~~–Also~~ the Code of Practice advises that in such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy.

The Council is not authorised to carry out intrusive surveillance.

3. **Covert use of Human Intelligence Source (CHIS)**

3.1 A person is a **Covert Human Intelligence Source** if:

- a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c).
- b) he covertly uses such a relationship to obtain information or provide access to any information to another person; or
- c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

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

3.3 A relationship is used covertly and information obtained is disclosed covertly, if and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

3.4 An example given by the Home office is where intelligence suggests a local shopkeeper is selling alcohol to underage customers and the local authority engages an employee to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited, that the authority can conclude that an authorisation is unnecessary.

3.5 **Lay Witnesses**

Choose carefully how you ask lay witnesses to gather information for you. -For example, if a member of the public telephones to complain about noise nuisance caused by a neighbour. -The lay witness~~third party~~ is in a relationship with the neighbour ~~at person~~ already and is just passing on information to the Council and would not be covered by RIPA. -However the more the Council tasks a lay witness to do something then you may inadvertently change them into a CHIS.

If you are in any doubt seek advice from an Authorising Officer, and if they are in doubt they will seek advice from the Senior Responsible Officer~~Solicitor~~.

3.6 **The Use of Covert Human Intelligence Sources**

3.6.1 In practice, it is most unlikely that it will ever be appropriate for the Council to utilise a CHIS. However, in the event that it is ever considered, advice should be sought from the Senior Responsible Officer~~Solicitor~~ at an early stage. -It is potentially possible, that the role of a Council employee may be that of a source, or the Council may also use an external or professional

source for the purpose of obtaining information. -Such persons may be a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b or c of paragraph 3.1.

3.6.2 Nothing in RIPA prevents material obtained by an employee acting as a source being used as evidence in Court proceedings.

3.6.3 The Authorising Officer must consider the safety and welfare of a CHIS acting as a 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 and considering what issues could be facing the security and welfare of a CHIS in relation to what they are to be asked to do. This should take place before any authorisation is granted, at any renewal, review and cancellation.

3.6.4 Before authorising the use of a CHIS as a source, the Authorising Officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. -He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). -Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

3.6.5 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, "confidential material" is likely to be obtained (see definition of confidential material in Appendix 1). -Special provisions relate to vulnerable individuals and juvenile services.

3.6.6 In addition to the usual authorisation process, the following management arrangements must be in place at all times in relation to the use of a CHIS:

1. there will be an appropriate officer of the Council (-'handler') who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS; and
2. there will be a second appropriate officer of the Council who has general oversight of the use made of the CHIS, and who will have responsibility for maintaining -an accurate and proper record about the source and tasks undertaken ->('manager' and 'recorder').

3.6.7 The CHIS forms contain appropriate boxes and prompts for ensuring the above is carried out.

4. Duration, Authorisations, Reviews, Renewals and Cancellations

4.1 Duration

4.1.1 Authorisations lapse, if not renewed

- 4.1.1.1 within 12 months –from date of last renewal if it is for the conduct or use of a covert human intelligence source or
- 4.1.1.2 in all other cases (i.e. directed surveillance) 3 months from the date of their grant or latest renewal.

4.1.2 Directed Surveillance - Authorisation

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

- a) that an authorisation is **necessary** (on the one the ground detailed below) and
- b) the authorised surveillance is **proportionate** to what is sought to be achieved by carrying it out.

4.1.2.2 An authorisation is necessary on the grounds stated below following the introduction of the Protection of Freedoms Act 2012:-

- a) for the purpose of preventing or detecting conduct which constitutes/corresponds to a criminal offence that is punishable by a maximum custodial sentence of 6 months or more or
- b) constitutes an offence under s.146, 147, or 147A of the Licensing Act 2003- selling alcohol to children or
- c) selling tobacco to persons under 18 years of age (s.7 Children and Young Persons Act 1933)

4.1.2.3 The Authorising Officer should set out, in his own words, why he believes the activity is necessary and proportionate. A bare assertion is insufficient. The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

- a) necessary for the ground stated above –and

be able to demonstrate the reasons why it is necessary and;

b) proportionate to its aim

This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary.

The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is important therefore that all officers involved in surveillance are fully aware of the extent and limits of the authorisation.

The Code of Practice [2014](#) gives an example of an individual suspected of carrying out a series of criminal damage offences at a local shop, after a dispute with the owner. It is suggested that a period of directed surveillance should be conducted against him to record his movements and activities for the purposes of preventing or detecting crime.

Although these are legitimate grounds on which directed surveillance may be conducted, the Home Office code states that it is unlikely the interference with privacy will be proportionate in the circumstances of the particular case. In particular, the obtaining of private information on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed..

- 4.1.2.4 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained. The applicant in completing the forms must provide facts and evidence
It is also sensible to make any authorisation sufficiently wide enough to cover the means required as well as being able to prove effective monitoring of what is done against what is authorised.
- 4.1.2.5 Authorisations must be in writing. The standard forms to be used can be accessed via the Council's intranet.
- 4.1.2.6 IMPORTANT NOTE: THE PROTECTION OF FREEDOMS ACT 2012 INTRODUCES A REQUIREMENT FOR MAGISTRATE APPROVAL FOR ALL RIPA AUTHORISATIONS FROM 1st NOVEMBER 2012. ACCORDINGLY AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A JP HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E. A GRANT OR RENEWAL. —The procedure and application process is set out in Annex A, B and C of Appendix 8. It is important that you seek advice from the Senior [Responsible OfficerSolicitor](#)—before making the application for judicial approval.
- 4.1.2.7 Any Authorising Officer proposing to approve an application for the use of directed surveillance or for the use of a covert human intelligence source must immediately inform the Senior [Responsible OfficerSolicitor](#)—who will then make arrangements for an application to be made to the Magistrates' Court.
- 4.1.2.8 In such circumstances, the Council will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if and only if, at the date of the grant of authorisation

or renewal of an existing authorisation they are satisfied that:

- (a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain.
- (b) the "relevant conditions" were satisfied in relation to the authorisation.

Relevant conditions include that:

- (i) the relevant person was designated as an Authorising Officer.
- (ii) it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with.
- (iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA (restrictions on the rank of the person granting the authorisation).
- (iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant or renewal of the authorisation, it may make an order to quash that authorisation. However the Court must not exercise its power to quash the authorisation unless the Council has had at least two business days from the date of the refusal in which to make representations.

4.1.3 **Reviews**

- 4.1.3.1 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.
- 4.1.3.2 It is recommended that regular reviews be undertaken to see if the need for the surveillance is still continuing. Results of reviews should be recorded in

the Central Register of Authorisations (see paragraph 7). -Reviews should be more frequent when access to confidential information or collateral intrusion is involved. -Review frequency should be as often as the Authorising Officer deems necessary or practicable.

4.1.3.3 Each Authorising Officer will therefore determine in each case how often authorisations should be reviewed. It is recommended that they ensure records of the review be supplied on the relevant form. Copies should be sent to the Senior SolicitorResponsible Officer –to keep the Central Register up to date.

4.1.4 **Renewals**

4.1.4.1 An Authorising Officer may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was given. A renewal of the authorisation in writing can be made for 3 months. Applications for renewal should detail how many times an authorisation has been renewed; significant changes to the original application for authority; reasons why it is necessary to renew; content and value of the information obtained so far and results of regular reviews of the investigation or operation.

4.1.4.2 Each application to renew should be made at least 7 days before the authorisation is due to expire on the relevant form. A record of the renewal should be kept within the applying service and supplied centrally to the Senior SolicitorResponsible Officer to be placed in the Central Register.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 RENEWALS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE RENEWAL. SEE PARAGRAPH 4.1.2.6 - 4.1.2.8 ABOVE.

4.1.5 **Cancellations**

4.1.5.1 All authorisations, including renewals should be cancelled if the need for the surveillance is no longer justified. This will occur in most cases where the purpose for which the surveillance was required has been achieved.

4.1.5.2 Requesting officers should ensure they inform Authorising Officers if this is the case before the next review. If, in the opinion of the Authorising Officer at

the next review, the need for surveillance is no longer justified, it must be cancelled.

- 4.1.5.3 The cancellation forms will be used to record a cancellation, and the Authorising Officer will ensure the original cancellation has been sent to the Senior Responsible Officer ~~Solicitor~~—or nominated representative to update the Central Register.

4.2 Covert Use of Human Intelligence Sources

4.2.1 Authorisation

- 4.2.1.1 The same principles as set out in paragraphs 4.1.2.1 and 4.1.2.2 apply to CHIS except the ground on which a CHIS can be authorised, which remains unaltered by the Protection of Freedoms Act 2012.

A CHIS authorisation can only be approved where it is necessary for the purpose of preventing or detecting crime, or of preventing disorder.

A CHIS authorisation can last for up to 12 months.

- 4.2.1.2 The conduct so authorised is any conduct that:

- a) is comprised in any such activities involving the conduct or 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.

- 4.2.1.3 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against what is authorised.

4.2.2 Renewals/Reviews

- 4.2.2.1 Similar provisions apply for a CHIS except that a

renewal here can last for a further 12 months, a review must have been carried out on the use of the source and an application should only be made to renew when the initial authorisation period is drawing to an end. Applications to renew a CHIS also should contain use made of the source and tasks given to the source during the previous authorised period and the information obtained.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E. A GRANT OR RENEWAL. SEE PARAGRAPH 4.1.2.6-4.1.2.8 ABOVE.

4.2.3 **Cancellations**

4.2.3.1 The same principles as Directed Surveillance apply.

4.2.3.2 Separate forms have been devised for applications to authorise, review, renew and cancel a CHIS. These can be accessed via the Council's intranet.

5. **Communications Data**

5.1 **Acquisition of Communications Data ~~Order 2010~~**

The Regulation of Investigatory Powers (Communications Data) Order 2010 replaced the earlier 2003 order which gave local authorities the powers set out within RIPA to access communications data. The 2010 Order raised the seniority of the Authorising Officers in local authorities to a 'Director, Head of Service, Manager or equivalent.' Communications data includes information relating to the use of a communications service but does not include the contents of the communications itself. Communications data can be split into three types; "traffic data" i.e. where a communication was made from, to whom and when; "service data" is the use made of the service by any person eg itemised telephone records; and "subscriber data" i.e. any other information that is held or obtained by an operator on a person they provide a service to. Local authorities are allowed to access "service data" and "subscriber data"; they are not allowed to access "traffic data".

~~NOTE: An Investigatory Powers Bill was announced in the Queen's Speech in May 2015 relating to communications data. The bill's progress will be monitored and amendments to this policy will be made as and when required..~~

5.2 **Authorisation**

The Order permits access to communications data, by local authorities

only where it is necessary for the purpose of preventing or of detecting crime or preventing disorder. —As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve. It should not be authorised where less intrusive means can be used to further an investigation

5.3 Alternative methods for authorisation

Access to communications data may be authorised in two ways; either (a) through an authorisation by an Authorising Officer which would allow the authority to collect or retrieve data itself, or (b) by a notice given to a postal or telecommunications operator requiring that operator to collect or retrieve the data and provide it to the local authority.

5.4 Application

Application will be made by the investigating officer and submitted to a Single Point of Contact (SPOC) who will either accept or reject the application. If the SPOC accepts the application he will forward it together with a SPOC report and a draft notice (where appropriate) to an Authorising Officer for authorisation.

If the Authorising officer accepts the application, it will need to be approved by a magistrate before the forms are returned to the SPOC and the SPOC will deal with the postal or telecommunications operator directly. The SPOC will also advise investigating officers and Authorising officers on whether an authorisation or a notice is appropriate in the circumstances.

Although it is unlikely that the Council will access communications data, in the event that it did, the Council would appoint a nominated SPOC from NAFN, (National Anti- Fraud Network), who have received training on a course recognised by the Home Office.

Authorising Officers

Authorising Officers for the purposes of communications data will be the same as for directed surveillance and CHIS's.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION. SEE PARAGRAPHS 4.1.2.6 - 4.1.2.8 ABOVE.

6. Other Factors to Consider

- 6.1** Particular consideration should be given to **collateral intrusion** i.e. the risk of intrusion into the privacy of those not directly the targets of the investigation. —Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who

are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests, as outlined above, apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. 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.

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

6.3 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subject 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.

6.4 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

6.5 **Confidential Material**

RIPA does not provide any special protection for **‘confidential material’** (see the definitions in Appendix 1). –Nevertheless, such material is particularly sensitive, and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation, i.e. by the chief Executive.

6.6 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.

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

➤ Those handling material from such operations should be alerted to

anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Senior ~~Solicitor~~ Responsible Officer 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 Senior ~~Solicitor~~ Responsible Officer) is satisfied that it is necessary for a specific purpose;
- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.
- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

6.8 In the case of confidential information a higher level of authorisation is required. —Therefore where authorisation is sought to carry out surveillance in respect of communications subject to legal professional privilege, or containing confidential personal information or confidential journalistic material, the Chief Executive must sign the authorisation.

6.9 Joint Working

In cases of joint working, where one agency is acting on behalf of another, usually the tasking agency can obtain or provide the authorisation i.e. if the Council has been tasked by the Police to assist in a covert surveillance operation, they should get the authorisation, which would then cover the Council. But advice should be sought from the Senior ~~Solicitor~~ Responsible Officer prior to any arrangements being agreed.

6.10 Handling and Disclosure of Materials

Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 6.7 above.

6.11 Applications and associated reviews, renewals and cancellations for directed surveillance shall be centrally retrievable 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.

6.12 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. If in doubt advice should be sought from the Senior ~~Solicitor~~ [Responsible Officer](#).

6.13 There is nothing in RIPA that prevents 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 ground, on which it was obtained, should be authorised only in the most exceptional circumstances. –Advice should be sought from the Senior ~~Solicitor~~ [Responsible Officer](#).

7. Central Register of Authorisation

7.1 The RIPA Code of Practice requires a central register of all authorisations to be maintained. –The Legal Section maintains this register.

7.2 Whenever an authorisation is authorised, renewed, reviewed or cancelled the Authorising Officer must send the signed original authorisation to the Senior ~~Solicitor~~ [Responsible Officer](#) or nominated representative. Receipt of the form will be acknowledged.

7.3 The Central Register will contain the following information:

- the type and date of authorisation
- the name and grade of the Authorising Officer
- a unique reference number for the investigation or operation
- the title of the investigation/operation, and a brief description and names of the subjects, if known
- if an authorisation is renewed, when and the name and designation of the Authorising Officer
- if confidential information is likely to be a consequence of the investigation or operation
- the date the authorisation was cancelled;
the date of magistrates court approval

7.4 The legal section will securely retain the original authorisations and maintain the Central Register. Authorisations should only be kept for a minimum of 5 years from the end of an authorisation. –Once the investigation is closed (bearing in mind cases may be lodged some time after the initial work) the records held by the department should be disposed of in an appropriate manner (e.g. shredded).

8. Codes of Practice

There are Home Office codes of practice and Office of Surveillance

Commissioners (OSC) Guidance that expand on this policy statement and copies are attached at Appendices 4 and 6. The Codes also lists General Best Practices, which should be followed where at all possible.

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”.

Staff should refer and familiarise themselves with the Home Office Codes of Practice and OSC Guidance for supplementary guidance.

Authorising Officers and the Senior Responsible Officer (~~Senior Solicitor~~) should also familiarise themselves with the Procedures and Guidance document produced by the OSC attached at Appendix 6.

9. Benefits of Obtaining Authorisation Under RIPA

9.1 Authorisation of surveillance and human intelligence sources

RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and
- the conduct is in accordance with the authorisation, then
- it shall be “lawful for all purposes”.

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

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

- a) is incidental to any conduct that is lawful by virtue of an authorisation; and
- b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

10 Scrutiny and Tribunal

10.1 The [Investigatory Powers Commissioner's Office \(IPCO\)](#) has taken over the inspection and oversight functions on RIPA which was

previously carried out by the Surveillance Commissioner's Office. Surveillance Commissioner will regulate conduct carried out under RIPA. The Surveillance IPCO Commissioner and his assistants will continue to ensure RIPA compliance by conducting are conducting a programme of inspections of Local Authorities. As a generality, they aim to inspect each council in England, Wales and Scotland once every three years but have introduced remote desktop inspections when a local authority has significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns. However, a desktop inspection will always be followed by an onsite inspection.

7

- 10.2** RIPA provides for the establishment of a tribunal to consider and determine complaints made under RIPA, and persons aggrieved by a local authority's conduct e.g. directed surveillance can make complaints to the tribunal. The forum hears applications 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 authorisation and can order destruction of any records or information obtained by such 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/all conduct as a result of such authorisation.
- A disclosure notice requirement is given.

11 Covert Surveillance of Social Networking Sites (SNS)

11.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist it in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public it serves. It is important that the council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need for RIPA authorisation; (use of the internet prior to an investigation should not normally engage privacy considerations).

11.2 If the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

- 11.3 Officers are required to follow the processes outlined in Appendix 11, when viewing social media sites in investigations— or to gather information..
- 11.4 The following guidance taken from the Home Office Covert Surveillance and Property Interference Revised Code of Practice (August 2018) is intended to assist -the Council in identifying when such authorisations may be appropriate.
- ~~The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.~~
- 11.5 The internet may be used for intelligence gathering and/or as a surveillance tool.
- 11.62 Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this policy.
- 11.7 Where an officer is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (see paragraph 3.6 -of this policy and paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice). -However, it is considered that it is most unlikely that it will ever be appropriate for the Council to utilise a CHIS.
- 11.8 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where the Council -has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be ~~available~~required.
- 11.9 As set out in paragraph 11.10 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain. However in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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

11.11 Whether -the council interferes with a person's private life includes a consideration of the nature of the -council's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a -council is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

11.12 **Example 1:** An officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: An officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3: An officer -undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or

operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

11.13 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake.

Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- 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 (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- 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
 - Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.
 - 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.
 - Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

Example: Officers using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group

are applied to the search or analysis, an authorisation should be considered.

~~- Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. However, where repeated viewings of open profiles on SNS is necessary and proportionate to gather further evidence or monitor an individual's profile or lifestyle, then RIPA authorisation must be considered as repeat viewing of "open source" sites may constitute directed surveillance and must be reviewed on a case by case basis.~~

- ~~11.3 If it is necessary and proportionate for the Council to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content). This will include entering into any online conversation or dialogue with a third party covertly, ie where they do not know the true identity of the person they are communicating with or the purpose of the communication. It could also include sending a 'friend request' on Facebook or joining a group, especially where any communication is transmitted to ensure the request is accepted...~~
- ~~11.4 It is not unlawful for Council officers to set up a false identity but it is inadvisable for a Council officer to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.~~
- ~~11.5 Council officers should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done.~~
- ~~11.6 To avoid the potential for inappropriate or inadvertent use of SNS in investigative and enforcement roles, Council officers should be mindful of the following:~~
- ~~● Do obtain the approval of your manager before accessing any SNS in accordance with the Council's Social Media and Employment Policy~~
 - ~~● If it is necessary and proportionate to breach covertly access~~

controls, the minimum requirement is an authorisation for directed surveillance.

~~• When viewing an individual's public profile on SNS, do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute an investigation~~

~~• Do not create a false identity in order to befriend individuals on SNS without authorisation under RIPA.~~

~~• Repeated viewings of open profiles on SNS to gather evidence or to monitor an individual's status, may constitute directed surveillance and must be reviewed on a case by case basis.~~

~~• A CHIS authorisation is required if entering into any online conversation or dialogue with a third party covertly.~~

~~• Be aware that it may not be possible to verify the accuracy of information on SNS and if such information is to be used as evidence, take reasonable steps to ensure its validity.~~

~~• During the course of an investigation, the nature of the online activity may evolve, therefore continually assess and review the activity to ensure it remains lawful and compliant with RIPA.~~

12 **Conclusion**

12.1 If you can carry out investigations in an obviously overt way so that it does not compromise what you are trying to achieve then that is the best way. However, if you need to do things covertly, then you need to consider RIPA and you are advised to take a broad wide view and interpretation of your activities. If you are in doubt you can seek advice from the Senior Responsible Officer~~Senior Solicitor~~ and remember if there is any doubt then it is usually safer to get an authorisation.

Definitions from the 2000 Act

- **“RIPA”** means the Regulation of Investigatory Powers Act 2000.
- **“Confidential Material”** consists of:
 - a) matters subject to legal privilege;
 - b) confidential personal information; or
 - c) confidential journalistic material
- **“Matters subject to legal privilege”** includes both oral and written communications between a professional legal adviser and his/her client or any person representing 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, and relating:
 - a) to his/her physical or mental health; or
 - b) to spiritual counselling or other assistance given or to be given, and

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

 - c) it is held subject to an express or implied undertaking to hold it in confidence; or
 - d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.
- **“Confidential Journalistic Material”** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.
- **“Covert Surveillance”** means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

- **“Authorising Officer”** means a person designated for the purposes of RIPA to grant authorisations for directed surveillance.

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

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

Extract from Part 7 of the Council's Constitution- Management Structure and Scheme of Delegation

Scheme of Delegation to Officers –

All delegations to officers are subject to the following general conditions:

(2) In the absence of the Chief Executive the functions of the Chief Executive will be the responsibility of either one of the three Service Directors

Executive Functions Delegated to the Chief Executive (7) To provide the necessary authorisations in respect of surveillance in accordance with the Regulation of Investigatory Powers Act 2000, where confidential information is involved or where authorisation is sought for the employment of a juvenile or vulnerable Covert Human Intelligence Source (CHIS).

Executive Functions Delegated to the Service Directors

(2) To act as authorising officers for the purposes of the Regulation of Investigatory Powers Act 2000 and Protection of Freedoms Act 2012.

Executive Functions Delegated to the [Legal Services Manager Senior Solicitor](#)

(3)To act as the Senior Responsible Officer for the purpose of Part II of the Regulation of Investigatory Powers Act 2000

(4) To make an application to a Justice of the Peace in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the Council in making such an application.

Executive Functions Delegated to Fraud and Compliance Manager and Fraud Investigation Officers

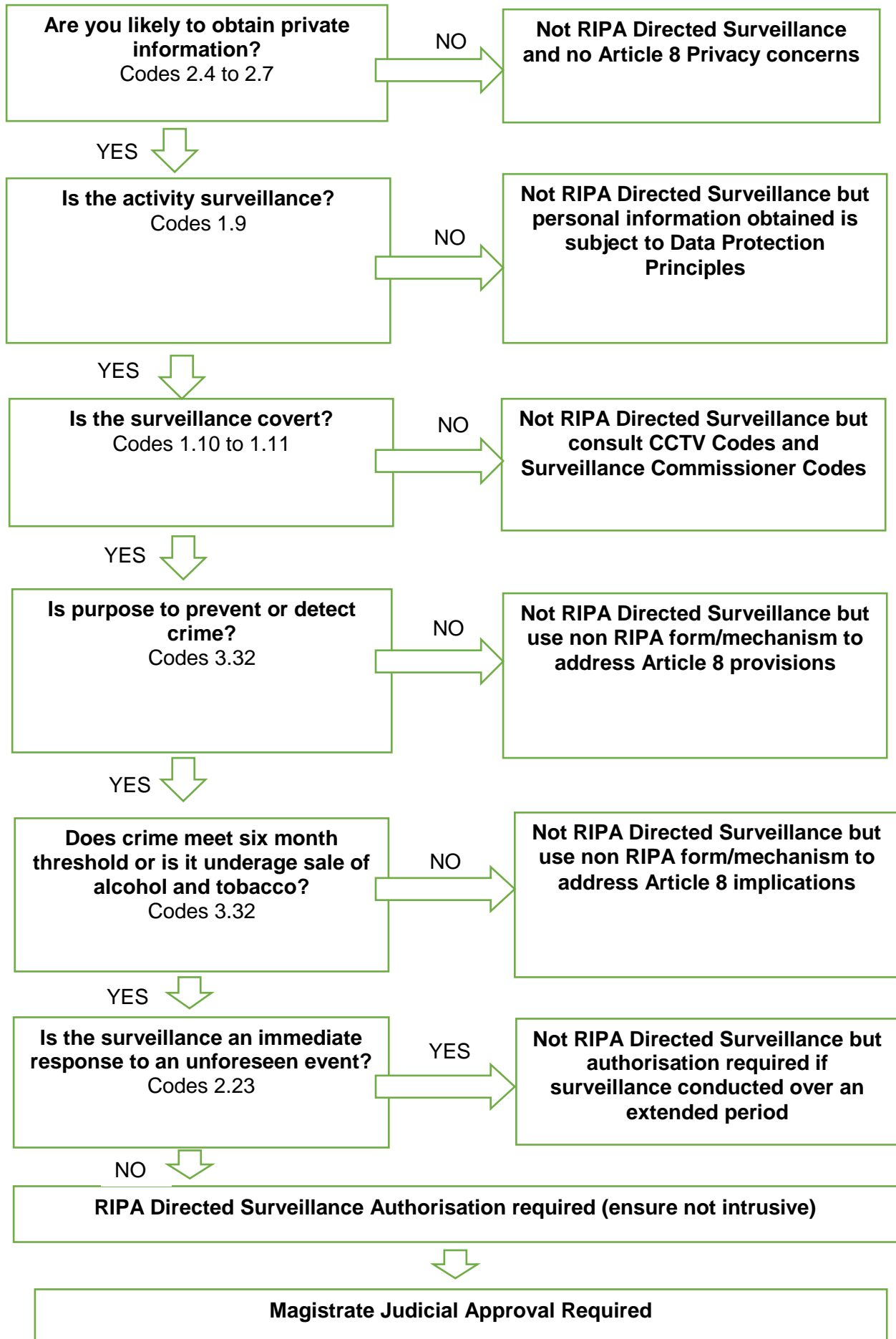
(1) To make an application to a Justice of the Peace, in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the Council in making such an application

(3)Power to carry out surveillance which is governed by the Regulation of Investigatory Powers Act 2000 as agreed by an authorising officer.

Examples of Surveillance

Examples of different types of Surveillance.	Examples
Surveillance that does not require RIPA Authorisation	<ul style="list-style-type: none"> - Council officers on patrol, who conceal themselves to observe suspicious persons that they come across in the course of a routine patrol. - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Sampling purchases (where the officer behaves no differently from a normal member of the public). - Dog Warden in uniform on patrol in park, street or van - Food Safety or Health & Safety Inspections -General observational duties not specifically targeted/planned or considered directed surveillance. . - CCTV cameras providing general traffic, crime or public safety information - Covert surveillance of an employee who is suspected by his employer of undertaking additional duties in breach of discipline regulations, as it does not relate to the discharge of the Employer's core functions.
Covert Directed Surveillance must be RIPA authorised.	Officers follow/observe an individual or individuals over a period, to establish whether s/he is working when claiming benefit provided the conduct constitutes/corresponds to a criminal offence punishable with at least 6 months imprisonment
Surveillance that is not intrusive	- An observation post outside residential premises, which provides a limited view compared to that which would be achievable from within the premises.
Intrusive – Council cannot do this!	<ul style="list-style-type: none"> - Planting a listening or other device in a person's home or in their private vehicle. - Use of a zoom lens outside residential premises, which consistently achieves imagery of the same quality as that which would be visible from within the premises.

RIPA Directed Surveillance Decision Chart for Local Authorities



PROCESS TO BE FOLLOWED WHEN CONSIDERING USING SOCIAL NETWORKING SITES IN INVESTIGATIONS OR TO GATHER EVIDENCE.

Where an officer considers it necessary to view a social networking site to investigate an allegation or to gather information the following process is to be followed:

- 1 Officers must not use their own personal or private account when accessing social networking sites for investigations/evidence gathering, only Council accounts should be used.
- 2 Officers may access the main page of an individual's profile to take an initial view as to whether there is any substance to the allegation of the matter being investigated and is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation.
- 3 Officers are required to keep a log recording when social networking sites are viewed for investigations/evidence gathering. Each viewing of a company or individual's social networking site must be recorded on the log. This is to enable the Council to monitor the use of these sites for investigations/evidence gathering and use this information to review policies and guidance.
- 4 If it is considered that there is a need to monitor a company's or individual's social networking site, for example by systematically collecting and recording information about a particular person or group, then the officer must refer the matter to their Head of Service for consideration as to whether a RIPA authorisation from the Magistrates Court may be required. If officers are in any doubt as to whether an authorisation is required, they should seek advice from the Senior Responsible Officer, (Mary Grimshaw), before continuing to access a social networking site.
- 5 If the offence being investigated falls under RIPA (see Paragraph 4.1.2.2 of the Council's RIPA policy), a formal RIPA application must be completed, authorised by one of the Council's Authorising Officers and then approved by a Magistrate.
- 6 If the offence being investigated falls outside RIPA, a 'Non-RIPA' form must be completed and forwarded to the Senior Responsible Officer.
- 7 Officers also need to be aware that any evidence captured as part of a criminal investigation will need to comply with the relevant legislation (The Police and

Criminal Evidence Act 1984, Criminal Procedure Rules 2018 and the Criminal Procedure and Investigations Act 1996) and advice should be sought from the Council's Legal Services Manager.

General guidance on RIPA/ Non- RIPA and appropriate forms can be found on the Council's intranet at:

<http://intranet/services/RIPA/Pages/>

<http://intranet/services/RIPA/Pages/Non-Ripa.aspx>