Appendix 1

Bromsgrove District Council

And

Redditch Borough Council

Regulation of Investigatory Powers Act 2000

Policy

Version 8.9

Document Control

Organisation	Bromsgrove District Council and Redditch Borough Council
Owner	Principal Solicitor
Protective Marking	Unclassified
Review Due	Annual. See Revision History for date of last update. This Policy is also reviewed by Council Members for approval each year in June.

Revision History

Revision Date	Revised By	Version	Description of Revision
Jan 2013	Sarah Sellers		Not recorded.
30/8/2013	Clare Flanagan	August 2013	• Document history page added. • References to 'urgent oral authority' removed. • Appendix 5 (about accessing Comms data) removed, now unnecessary.
1/9/2013	Clare Flanagan	August 2013	Update to Appendix 2 to remove all 'grounds for use' except prevention of crime.
28/8/2015	Nicola Brothwell	V4.0	Version numbering introduced. Removal of mention of staff who have left the Council.
19/1/2016	Nicola Brothwell	V5.0	Minor updates to list of Authorising Officers. OSC guidance on use of social media added.

Revision Date	Revised By	Version	Description of Revision
18/5/2016	Nicola Brothwell	V6.0	Chris Phillips has now left the council, so his name is removed from the policy.
10/04/2017	Sarah Sellers	V7.0	Amalgamated polices of both BDC and RBC into one policy. Updated advice on use of social media and use of non-RIPA surveillance.
11/01/2019	Nicola Brothwell	V7.1	Change authorisation period for juvenile CHIS from 1 to 4 months. IPCO has taken over from IOCCO and OSC, so all references updated.
4/02/2019	Nicola Brothwell	V7.2	Liz Tompkin removed as an Authorising Officer.
16/6/2020	Nicola Brothwell	V7.3	Addition of section ‘Obtaining Communications Data
3/9/2020	Nicola Brothwell	V7.4	‘Review Due’ field added to Document Control Section.
18/11/2021	Nicola Brothwell	V8.0	New SRO. Changes in line with IPCO requirements outlined in letter 2020, new Data safeguards section in this Policy. RIPA forms removed from Policy. General review re changes required by UK leaving the EU.

Revision Date	Revised By	Version	Description of Revision
1/7/2022	Nicola Brothwell	V8.1	Change of SRO Inclusion in CHIS section of relevant text regarding Public Volunteers, from Covert Human Intelligence Sources Code of Practice 2018. Inclusion in Social Media section of relevant text from Covert Surveillance and Property Code of Practice. Update mention of quarterly RIPA meetings to six-monthly meetings.
18/7/2022	Nicola Brothwell	V8.2	In Data safeguards section, added a timescale for reviews of documentation to comply with the Inspector's recommendation.
14/5/2024	Nicola Brothwell	V8.3	Authorised Officer list updated (removed Kevin Dicks, added Peter Carpenter, and updated Sue Hanley's job title)
1/8/2024	Nicola Brothwell	V8.4	Use of Social Media section updated to remove mention of OSC and IPCO guidance.
24/3/2025	Nicola Brothwell	V8.5	Update RBC logo on cover page. Update job title, Claire Felton. Authorised Officer list updated (removed Sue Hanley and Peter Carpenter, added John Leach and Bob Watson)
27/5/2025	Nicola Brothwell	V8.6	IPCO suggested updates from inspection April/May 2025. Deb Poole removed from list of Authorised Officers.

Revision Date	Revised By	Version	Description of Revision
27/8/2025	Nicola Brothwell	V8.7	Replace mention of Twitter with ‘X’. Appendix 2 flowchart – wording now outdated (refers to Her Majesty). Added accompanying wording.
22/5/2026	Nicola Brothwell	V8.8	Removed Bob Watson from list of Authorising Officers, added James Walton. Updated Authorising Officer contact telephone numbers.
1/10/2026	Nicola Brothwell	V8.9	Removed Simon Wilkes from the list of Authorising Officers, added Mark Cox, and updated contact details. Also removed header hyperlink and replaced with text, to solve problem with modern.gov uploading the Policy.

Contents

Introduction 9

What are the origins of RIPA? 10

When does RIPA apply and who does it apply to? 11

The Human Rights Act 1998 12

Definition of core functions 12

Private information 13

What happens if RIPA is ignored? 13

Surveillance outside of RIPA 14

What is surveillance? 14

Surveillance 14

Covert surveillance 14

Directed surveillance 15

Immediate response to events 15

Recording of telephone conversations 15

Intrusive surveillance: 15

Commercial premises and vehicles 16

Covert Human Intelligence Source (CHIS) 16

Conduct and use of a source 17

Management of sources 17

Tasking 18

Management responsibility 18

Security and welfare 18

Persons who repeatedly provide information 19

Public Volunteers 19

Record management for CHIS 21
RIPA application and authorisation process 22
Application, review, renewal and cancellation forms 22
Applications 25
Duration of applications 25
Reviews 26
Renewal 26
Cancellation 27
Who can grant a RIPA authorisation? 28
Urgent oral authorisations 28
Local sensitivities 28
Authorising officers' responsibility 28
Necessity and proportionality 29
Collateral intrusion 30
Unexpected interference with third parties 31
Confidential information 31
Use of CCTV 32
Use of Social Media 32
Obtaining Communications Data 35
Joint agency surveillance 37
Documentation and central record 37
Annual report to Investigatory Powers Commissioner's Office 39
Storage and retention of material 39
Data safeguards 39
Evidence 40

Reviews 40
Dissemination of information 40
Copying 41
Storage 41
Destruction 41
Confidential or privileged information 41
Items subject to legal privilege 42
Covert surveillance of legal consultations 42
Lawyers' material 42
Handling, retention, and deletion of legally privileged material 42
Training 43
Oversight 43
Reporting to members 44
Scrutiny and tribunal 44
Appendix 1 45
Appendix 2 46

Introduction

The purpose of this policy is to explain the scope of Regulation of Investigatory Powers Act 2000 and the circumstances where it applies to the Council. It provides guidance on the authorisation procedures to be followed in the event that you need to undertake surveillance, setting it into context so that its importance may be appreciated.

The subject covered by this policy is complicated but of major importance. If, having read this document, you are unclear about any aspect of the process, or you have questions which are not answered explicitly by the content of this document, these should be referred either to one of the Authorising Officers or to the Assistant Director of Legal, Democratic and Procurement Services for assistance.

If, having taken advice, doubt exists as to whether the circumstances require an authorisation for consideration under this legislation, you should submit an application form to be authorised. This will demonstrate to any examining body that Bromsgrove District Council / Redditch Borough Council have taken their responsibilities seriously with regards to the protection of a person's privacy against the need for the activity to take place in operational terms. If you do not secure an authorisation it leaves any evidence gathered open to challenge under section 78 of the Police and Criminal Evidence Act 1984 (PACE,) as amended, as well as challenges for breach of privacy against the Council.

To assist with oversight of the Council's RIPA processes Claire Felton, Assistant Director of Legal, Democratic and Procurement Services, has been appointed as the Senior Responsible Officer who will be responsible for the integrity of the process. However it must be stressed that all staff involved in the process must take their responsibilities seriously. This will assist with the integrity of the Council processes and procedures.

On advice from the OSC (now superseded by the IPCO), and to reflect the operation of shared services across the two organisations, the separate RIPA policies for Bromsgrove District Council (BDC) and Redditch Borough Council (RBC) have been merged into one single policy. References made to "the Council" should be read as references to either BDC or RBC as the context requires.

Claire Felton

Assistant Director, Legal, Democratic and Procurement Services

Bromsgrove District Council and Redditch Borough Council

Updated: July 2022, reviewed September 2026

What are the origins of RIPA?

The Human Rights Act 1998 brought into UK law many of the provisions of the 1950 European Convention on Human Rights and Fundamental Freedoms. Article 8 requires the Council to have respect for people's private and family lives, their homes, and their correspondence. These subjects can be referred to as "Article 8 rights".

The Human Rights Act makes it unlawful for any local authority to act in a way which is incompatible with the European Convention on Human Rights. However, these are not absolute rights and there is a specific qualification giving the Council the ability to interfere with a person's Article 8 rights to the effect that:-

Such interference is in accordance with the law if:

- is **necessary**
- and is **proportionate**

These three points are clarified further in the next paragraphs.

When we talk of interference being "in accordance with the law", this means that any such interference is undertaken in accordance with the mechanism set down by the Regulation of Investigatory Powers Act (RIPA for short) and the Home Office Covert Surveillance Codes of Practice. The Codes of Practice deals with the use of Covert Surveillance and the use of persons such as informants and Undercover Officers who gather information in a covert capacity (Covert Human Intelligence Source or CHIS for short – refer to Page 16).

However a considerable amount of observations are carried out in an overt capacity by Council employees carrying out their normal functions such as parking enforcement, general patrolling etc. These activities are general and routine and do not involve the systematic surveillance of an individual. RIPA is not designed to prevent these activities or regulate them.

The Council has numerous statutory duties and powers to investigate the activities of private individuals and organisations within its jurisdiction for the benefit and protection of the greater public. Some of these investigations may require surveillance or the use of a CHIS. These may include

- benefit fraud
- environmental health
- housing
- planning
- criminal investigations by audit such as fraud offences

RIPA aims to provide a framework to control and supervise covert activities such as surveillance and the use of a CHIS in these criminal investigations. It aims to balance the need to protect the privacy of individuals against the need to protect others by the Council carrying out its enforcement functions. There are two separate codes of practice:

- Covert Surveillance and Property Interference
- CHIS

Any covert activity carried out under this legislation must meet the test of necessity and proportionality as set out in this policy. .

When does RIPA apply and who does it apply to?

RIPA applies to Public Authorities such as Local Authorities and permits them to conduct Covert Surveillance activities and use Covert Human Intelligence Sources (CHIS) such as informants and undercover officers (see pages 14 and 16) However, on 1 November 2012 two significant changes came into force that affect how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

The crime threshold, as mentioned is only for Directed Surveillance.

The only lawful reason for Local Authorities to conduct activity under RIPA is **prevention and detection of crime** in respect of its Core Functions. As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour unless there are criminal offences involved which attract a maximum custodial sentence of six months.

As a local authority Bromsgrove District Council and Redditch Borough Council and its staff have a responsibility to adhere to the RIPA legislation and the Human Rights Act.

In addition to applying to all staff employed by the two Councils who are engaged in activities that involve the protection and detection of crime, the policy will also apply to the following categories of staff:

- Contract or agency staff working at Bromsgrove District Council / Redditch Borough Council undertaking such activity as is covered by the RIPA and associated legislation and guidance.

- From 01 June 2010 all staff who are employed by Bromsgrove District Council as part of the Worcestershire Regulatory Services.

- All staff employed by Redditch Borough Council but whose duties include performing services for Bromsgrove District Council under any secondment arrangements or under section 113 of the Local Government Act 1972.

- All staff employed by Bromsgrove District Council but whose duties include performing services for Redditch Borough Council under any secondment arrangements or under section 113 of the Local Government Act 1972.

The Human Rights Act 1998

The RIPA Codes of Practice state where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Public authorities are therefore strongly recommended to seek an authorisation under RIPA where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Definition of core functions

Recent case law has established that a public authority may only use the powers under the 2000 Act when in performance of its core functions. These are defined by section 28(3) of the 2000 Act. It has been held that disciplinary investigations are ordinary functions whereas the investigation of benefit fraud would be a core function. Using the RIPA application and monitoring process when exercising core functions assists with protecting the Council from challenges under section 78 of PACE. However, surveillance in the case of serious disciplinary issue would be outside of RIPA. Any type of surveillance outside of RIPA should still meet the same tests of necessity and proportionality and advice should be sought from Legal Services prior to any such surveillance taking place.

Private information

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 surveillance, a directed surveillance authorisation may be considered appropriate.

If you need to conduct surveillance or use a CHIS as part of investigating a criminal matter which might result in court proceedings or proceedings before some other form of tribunal, you should consider whether private information is likely to be gained as a result of the activities and whether RIPA applies.

What happens if RIPA is ignored?

If Investigators undertake covert activity to which this legislation applies without the relevant authority being obtained and the case progresses to criminal proceedings, the defence may challenge the validity of the way in which the evidence was obtained under Section 78 of PACE. Should the evidence then be disallowed by a court, the prosecution case may be lost with a financial cost to the Council.

The person who was the subject of your surveillance may complain to the Ombudsman who may order the Council to pay compensation. The activity may also be challenged through the civil courts under the Human Rights Act 2000 for breach of privacy.

There is also a requirement to report errors to the Investigatory Powers Commissioner's Office or IPCO (formerly the OSC), such as surveillance activity which should have been authorised but which was carried out outside of RIPA. (See section on errors)

A properly obtained and implemented authorisation under RIPA will provide the Council with lawful authority to interfere with the rights of the individual. It is not simply enough that an authorisation for surveillance is obtained. It must be properly obtained, implemented, managed, reviewed and cancelled.

Surveillance outside of RIPA

As explained earlier there may be a necessity for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation such as in cases of serious disciplinary investigations. The Council still must meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented.

There is a requirement for the Councils' Senior Responsible Officer (SRO) to regularly monitor surveillance outside of RIPA. Therefore before any such surveillance takes place, advice must be sought from the Assistant Director of Legal, Democratic and Procurement Services or the Principal Solicitor.

What is surveillance?

Surveillance

Surveillance is defined in paragraph 1.9 of the Revised Codes of Practice as:

Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Covert surveillance

Covert Surveillance is defined in paragraph 1.10 of the Revised Codes of Practice as:

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

If activities are open and not hidden from the persons subject to surveillance, such as Officers conducting Council business openly, e.g. a market inspector walking through markets, the RIPA framework does not apply because that is "Overt Surveillance". Equally, if you tell the subject that surveillance may take place, the surveillance is overt.

RIPA does not regulate Overt Surveillance. However, remember the Council's responsibilities to ensure that whatever action is taken is compliant with the Human Rights Act and is a necessary and proportionate response to the issue being dealt with.

RIPA regulates two types of Covert Surveillance which are

- **Directed Surveillance**
- **Intrusive Surveillance**

Directed surveillance

Directed Surveillance is defined in paragraph 2.2. of the Revised Codes of Practice as:

Surveillance is directed surveillance if the following are all true:

- 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.

Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

Immediate response to events

There may be occasions when officers come across events unfolding which were not pre-planned which then require them to carry out some form of observation. This will not amount to Directed Surveillance. However it will amount to surveillance outside of RIPA and must still be necessary and proportionate and take account of the intrusion issues. As there is no provision to obtain an urgent oral authorisation it is important that officers do not abuse the process and they must be prepared to explain their decisions in court should it be necessary. Therefore they should document their decisions, what took place and what evidence or information was obtained.

Recording of telephone conversations

The recording of telephone conversations connected to criminal investigations (outside of the Councils monitoring at work policy with its own equipment) falls under RIPA which provides that where one party to the communication consents to the interception, it may be authorised in accordance with section 48(4) of the 2000 Act. In such cases, the interception is treated as directed surveillance.

There may be occasions where this is required such as a witness who has text or voicemail evidence on their mobile telephone and we need to examine the phone.

Intrusive surveillance:

Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

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

- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Local authorities are not permitted to carry out Intrusive Surveillance.

Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device 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. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

A risk assessment should be carried out of the capability of equipment being used when filming residential premises and private vehicles to ensure that the activity does not meet the criteria of Intrusive Surveillance.

Commercial premises and vehicles

Commercial premises and vehicles are therefore excluded from the definition of intrusive surveillance. However they are dealt with under the heading of Property Interference contained within the Police Act 1997.

Bromsgrove District Council/ Redditch Borough Council has no authority in law to carry out Intrusive Surveillance or activity under the Police Act 1997.

Covert Human Intelligence Source (CHIS)

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However the provisions of the 2000 Act are not intended to apply in circumstances 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 such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources unless they repeatedly provide information about particular issues, which is covered later in this section of the policy.

Under section 26(8) of the 2000 Act a person is a source if:

— they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

— they covertly use such a relationship to obtain information or to provide access to any information to another person; or

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

By virtue of section 26(9)(b) of the 2000 Act 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 the purpose.

By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above 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.

Conduct and use of a source

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

The **conduct of a source** is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfill whatever tasks are given to them or which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

When completing applications for the use of a CHIS you are stating who the CHIS is, what they can do and for which purpose.

When determining whether a CHIS authorisation is required, consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

Management of sources

Within the provisions there has to be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**

(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**

At all times there will also be a person who will have responsibility for maintaining a record of the use made of the source.

The **Handler** will have day to day responsibility for:

- dealing with the source on behalf of the authority concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and

- monitoring the source's security and welfare;

The Controller will be responsible for the general oversight of the use of the source.

Tasking

Tasking is the assignment of activity to the source by the Handler or Controller by, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

In some instances, tasking will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of the contents of the CHIS codes of Practice.

Management responsibility

Bromsgrove District Council/ Redditch Borough Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary, the CHIS Codes of Practice should be consulted by those considering the use of such tactics to ensure that the Council can meet its management responsibilities under the Code.

Security and welfare

The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

Persons who repeatedly provide information

It is possible that members of the public repeatedly supply information to Council staff on either one particular subject or investigation or a number of investigations. It is important that Council staff make the necessary enquiries with the person reporting the information to ascertain how the information is being obtained. This will not only assist with evaluating the information but will determine if the person is establishing or maintaining a relationship with a third person to obtain the information, and then provide it to the Council staff. If this is the case, the person is likely to be acting as a CHIS and there is a potential duty of care to the individual which treating them as a duly authorised CHIS would take account of. Therefore Council staff should ensure that they are aware of when a person is potentially a CHIS by reading the below sections. If further advice is required contact the RIPA Coordinating Officer.

Public Volunteers

The following extract from the CHIS Code of Practice is included to assist in understanding when public volunteers may become covert human intelligence sources (CHIS).

> 2.21 In many cases involving human sources, the source will not have established or maintained a relationship for a covert purpose. Many sources provide information that they have observed or acquired other than through a relationship. This means that the source is not a CHIS for the purposes of the 2000 Act and no CHIS authorisation is required.
>
> Example 1: 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 is not a CHIS. They are not passing information obtained as a result of a relationship which has been established or maintained for a covert purpose.
>
> Example 2: 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.
>
> 2.22 Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 are required to report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

2.23 Any such professional or statutory disclosures should not usually result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of obtaining or disclosing such information.

2.24 Tasking a person to obtain information covertly may result in a CHIS authorisation being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought, or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: 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 2000 Act, for example, a directed surveillance authorisation, may need to be considered where the activity is likely to result in the public authority obtaining information relating to a person's private or family life.

2.25 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.26 Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS, either expressly or implicitly, without obtaining a CHIS authorisation or considering whether it would be appropriate to do so.

Example: 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 established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining or 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.

2.27 It is possible that a person may become engaged in the conduct of a CHIS without a public authority inducing, asking, or assisting the person to engage in that conduct. However, a CHIS authorisation should be considered, for example, where a public authority is aware that an individual is independently maintaining a relationship (i.e.

"self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.

Record management for CHIS

Proper records must be kept of the authorisation and use of a source. The particulars to be contained within the records are;

a. the identity of the source;

b. the identity, where known, used by the source;

c. any relevant investigating authority other than the authority maintaining the records;

d. the means by which the source is referred to within each relevant investigating authority;

e. any other significant information connected with the security and welfare of the source;

f. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

g. the date when, and the circumstances in which, the source was recruited;

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

i. the periods during which those persons have discharged those responsibilities;

j. the tasks given to the source and the demands made of him in relation to his activities as a source;

k. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

l. the information obtained by each relevant investigating authority by the conduct or use of the source;

m. any dissemination by that authority of information obtained in that way; and

n. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Please refer to the section headed “Documentation and Central Record” (page 37) for further information regarding the holding of records relating to CHIS sources/ authorisations by the Information Management Team.

RIPA application and authorisation process

On 1 November 2012 two significant changes came into force that affects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (“the 2010 Order”) mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

This crime threshold, as mentioned, is only for Directed Surveillance.

Application, review, renewal and cancellation forms

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP’s approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows:-

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP’s approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of

the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing. The hearing will be in private and heard by a single JP.

Details of how to contact the local Courts for out of hours applications will be circulated to managers to be passed on to staff when required.

Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. The list of officers currently authorised can be found on the RIPA page of Orb. For further authorisations please contact the RIPA Coordinating Officer.

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA authorisation form, together with any supporting documents setting out the case, and the original authorisation form.

The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA authorisation and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**. However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**.

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to:

- Approve the Grant or renewal of an authorisation
- Refuse to approve the grant or renewal of an authorisation
- Refuse to approve the grant or renewal and quash the authorisation

Approve the Grant or renewal of an authorisation

The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the surveillance requested.

Refuse to approve the grant or renewal of an authorisation

The RIPA authorisation will not take effect and the local authority may **not** use the surveillance requested in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation

This applies where the JP refuses to approve the authorisation or renew the authorisation and decides to quash the original authorisation. However the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the Legal team who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date. The officers are now allowed to undertake the activity.

The original RIPA authorisation form and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and by the AO. This will enable the AO to check what was authorised and monitor any reviews and cancellation to determine if any errors occurred and if the objectives were met.

There is no complaint route for a judicial decision unless it was made in bad faith. If the applicant has any issues they must contact the Legal Department for advice. A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal team will review the case and consider what action, if any, action should be taken.

All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available from the Intranet site and the Information Management

Team, but officers must ensure that the circumstances of each case are accurately recorded on the application form.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference (see collateral intrusion on page 30). The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team, in order that they are aware of the activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However they should not be involved in the sanctioning of the authorisation. Completed application forms are to be initialed by Line Managers to show that the quality check has been completed.

Applications whether authorised or refused will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations. To obtain this number please contact Information Management Team on 01527 64252 ext. 1661.

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP's approval (see procedure above RIPA application and authorisation process).

Duration of applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Juvenile Sources	4 Months

Renewal	12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire (see cancellations page 27).

Reviews

The reviews are dealt with internally by submitting the review form to the authorising officer. There is no requirement for a review form to be submitted to a JP.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably or the techniques to be used are now different, a new application form should be submitted and will be required to follow the process again and be approved by a JP. If in doubt seek advice. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months.

Should it be necessary to renew a Directed Surveillance or CHIS authorisation, this must be approved by a JP.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the Authorising officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraph 5.24 in the Codes of Practice). **You must record the amount of time spent on the surveillance.**

The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issue instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Who can grant a RIPA authorisation?

Officers who are designated "Authorising Officers" may authorise the use of directed surveillance or the use of a CHIS.

Please refer to Appendix 1 for the list of Authorising Officers, to show name, departmental details, contact number and levels of Authority.

The Chief Executive Officer or in their absence the Deputy Chief Executive will authorise cases where confidential information is likely to be gathered or in the case of a juvenile or vulnerable CHIS.

The Assistant Director of Legal, Democratic and Procurement Services will inform the Information Management Team of any changes to the list of Authorising Officers and will amend the policy accordingly. The intranet will also be updated appropriately.

Urgent oral authorisations

As from 1 November 2012 there is now no provision under RIPA for urgent oral authorisations.

Local sensitivities

Authorising Officers and Applicants should be aware of particular sensitivities in the local community where the directed surveillance is taking place, or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. This should form part of the risk assessment.

It should be noted that although this is a requirement there is no provision made within the application form for this information. Therefore applicants should cover this area where they feel it is most appropriate such as when detailing the investigation or proportionality or within the separate risk assessment form. However it must be brought to the attention of the Authorising Officer when deciding whether to authorise the activity.

Authorising officers' responsibility

Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable such as where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the Central Record of authorisations (see page 37) should highlight this and it should be brought to the attention of a Commissioner or Inspector should his next inspection.

Authorising Officers must treat each case individually on its merits and satisfy themselves that the authorisation is in accordance with the law, **necessary** for the prevention and detection of crime, that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

The Authorising Officer must believe the surveillance is **proportionate** to what it seeks to achieve, taking into account the **collateral intrusion** issues, and that the level of the surveillance is appropriate to achieve the objectives. If any equipment such as covert cameras or video cameras are to be used, the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

Authorising Officers are responsible for determining when reviews of the activity are to take place (see Reviews on page 26).

Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should the Authorised Officer approve any RIPA form unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed.

Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

In the absence of your particular Line Manager or Assistant Director of Department the application should be submitted to another Authorising Officer for authorisation (see list of Authorising Officers - Appendix 1).

Necessity and proportionality

Obtaining a RIPA authorisation will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

It must be necessary for the **prevention and detection of crime and that** the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. It must also be shown the reasons why the requested activity is necessary in the circumstances of that particular case. Can you achieve the same end result without the surveillance?

If similar objectives could be achieved by methods other than covert surveillance, then those methods should be used before resorting to surveillance methods, unless it can be justified why they cannot or should not be used.

Then, if the activities are **necessary**, the person granting the authorisation must believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the subject 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. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.

The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.

The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

- 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 to be adopted 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 that the staff involved in the surveillance and the line manager manage the enquiry and operation, and constantly evaluate the need for the activity to continue.

Collateral intrusion

Collateral intrusion is an integral part of the decision making process and should be assessed and considered very carefully by both applicants and Authorising Officers.

The Revised Codes state Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation such as neighbours or other members of the subject's family. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance activity should be carefully considered against the necessity and proportionality criteria.

Intended intrusion could occur if it was necessary to follow a person not committing any offences but by following this person it would lead you to the person who is committing the offences.

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 apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

Prior to and during any authorised RIPA activity, a risk assessment should take place to identify the likely intrusion into the subject and any collateral intrusion. Officers should take continuing precautions to minimise the intrusion where possible. The collateral intrusion, the reason why it is unavoidable and your precautions to minimise it will have to be detailed on any relevant application forms. This will be considered by the Authorising Officer.

Before authorising surveillance the Authorising Officer should take into account the risk of collateral intrusion detailed on the relevant application forms as it has a direct bearing on the decision regarding proportionality.

The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but you should weigh up the importance of the activity to be carried out in operational terms on the one hand and the risk of collateral intrusion on the other hand.

Unexpected interference with third parties

When you are carrying out covert directed surveillance or using a CHIS, you should inform the Authorising Officer if the 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. It will be appropriate in some circumstances to submit a review form and in other cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

Confidential information

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material and applications where there is a likelihood of acquiring such information can only be authorised by the Chief Executive or the Executive Director of Services.

No authorisation should be given if there is any likelihood of obtaining legally privileged material without consulting the shared BDC/ RBC Legal Team.

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. Journalistic material is also mentioned in the codes however it is highly unlikely that this will be obtained. The definition should it be required can be obtained from the Codes of Practice at Chapter 4.

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

- Those handling material from such operations should be alert to anything which 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 Assistant Director of Legal, Democratic and Procurement Services before further dissemination takes place;

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

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Assistant Director of Legal, Democratic and Procurement Services) 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.

Use of CCTV

The use of the CCTV systems operated by the Council does not normally fall under the RIPA regulations. However it does fall under the Data Protection Act 1998 and the Councils CCTV policy**.** However should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or a copy of the authorisation page. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the Information Management Team for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

Use of Social Media

This part of the policy covers the use of social media, including Social Networking Sites (SNS) such as X (formerly Twitter) and Facebook, and selling platforms such as eBay and Gumtree.

It is taken as good professional practice in relation to covert surveillance of SNS that repeat viewing of individual ‘open source’ sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity.

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 social networking site 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.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information from their social media sites 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.

Where privacy settings are available but not applied the data may be considered ‘open source’ and an authorisation is not usually required. However, repeat viewing of ‘open source’ sites may constitute directed surveillance on a case by case basis and officers need to be aware of this and seek advice about obtaining an authorisation. For example if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance.

If it is necessary and proportionate for the Council to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance.

Officers also need to be aware that if viewing of on-line information progresses to an officer establishing a relationship whether through a friend request or sending an email purporting to be interested in an item to purchase, then a CHIS authorisation will be required. In that scenario the officer themselves would be regarded as acting as a CHIS. Using a third party to contact the subject on behalf of the Council would also require authorisation of the third party as a CHIS.

It is not unlawful for a council officer to set up a false identity, but this should not be done for a covert purpose without significant management consideration and under the control of an authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

To further assist in understanding matters pertaining to the use of social media in investigations, the following is included in this policy, from the Covert Surveillance and Property Interference Code of Practice 2018:

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their 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. But 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. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. 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 code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 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 19 no further steps are taken to conceal the activity. Conversely, where a public authority 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.

3.13 As set out in paragraph 3.14 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.

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

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority'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 public authority 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. See also paragraph 3.6. Example 1: A police 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: A customs 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: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or 20 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.

3.16 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 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.

3.17 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 (see paragraph 4.32). Example: Researchers within a public authority 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 by public authorities 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 21 or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

Obtaining Communications Data

The Investigatory Powers Act 2016 governs the lawful obtaining of communications data by public authorities. The term communications data includes the 'who', 'when', 'where', and 'how' of a communication but not the content, that is, what was said or written. A local authority cannot make an application that requires the processing or disclosure of internet connection records for any purpose.

Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, that is, postal services or telecommunications

services. All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories of entity data and events data.

Examples of entity data include:

- ‘subscriber checks’ such as “who is the subscriber of phone number 01234 567 890?”, “who is the account holder of email account example@example.co.uk?” or “who is entitled to post to web space www.example.co.uk?”

- subscribers’ or account holders’ account information, including names and addresses for installation, and billing including payments method(s), details of payments;

- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.

Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

- information identifying the sender or recipient of a communication from data comprised in or attached to the communication;

- itemised timing and duration of service usage (calls and/or connections);

- information about amounts of data downloaded and/or uploaded;

Part 3 of IPA contains provisions relating to authorisations for obtaining communications data. This part of IPA is now in force but the acquisition of communications data was previously covered by RIPA. Under RIPA, local authorities were required to obtain judicial approval in order to acquire communications data. However, the position has now changed and from June 2019, all communication data applications must instead be authorised by the Investigatory Powers Commissioner’s Office.

The Home Office issued ‘Communications Data’ Code of Practice in November 2018 and chapter 8 covers local authority procedures. A local authority must make a request to obtain communications data via a single point of contact (SPoC”) at the National Anti-Fraud Network (“NAFN”). In addition to being considered by a NAFN SPoC, an officer within the local authority of the rank of service manager or above should be aware the application is being made before it is submitted to an authorising officer in the IPCO.

A serious crime threshold applies to the obtaining of some communications data. The Council can only submit an application to obtain events data for the investigation of a criminal offence capable of attracting a sentence of 12 months or more. However, where the Council is looking to obtain entity data this can be done for any criminal investigation where it is necessary and proportionate to do so.

Joint agency surveillance

In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

Council staff involved with joint agency surveillance must ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity. When staff are operating on another organisations authorisation, they should obtain either a copy of the application form (redacted if necessary) or a copy of the authorisation containing the unique number. This will ensure they see what activity they are authorised to carry out. Their line manager should be made aware of the joint surveillance and a copy of the authorisation forwarded to the central register in order that a record can be retained. This will assist with oversight of the covert activities undertaken by Council staff.

Provisions should also be made regarding any disclosure implications under the Criminal Procedures Act (CPIA) and the management, storage and dissemination of any product obtained.

Documentation and central record

Authorising Officers or Managers of relevant enforcement departments must keep whatever records are necessary to administer and manage the RIPA application process, in compliance with the requirements of the Codes of Practice as reflected in the Safeguarding Policy. The Council holds a centrally held and retrievable record, also in compliance with the Codes of Practice.

This record will be held by the Information Management team and regularly updated whenever an authorisation is refused, granted, renewed or cancelled.. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request.

All original surveillance Authorisations and copies of judicial applications/order forms (whether authorised or refused), Review, Renewal and Cancellation documents will be forwarded electronically to the Information Management team for security purposes. The Information Management team will be responsible for maintaining the Central Record of Authorisations and will ensure that all records are held securely with no unauthorised access. The only persons who will have access to these documents will be the Information Management team, the Senior Responsible Officer and the RIPA Co-ordinating Officer. The Assistant Director of the shared Regulatory Service will have access to a read only copy of the Central Record of Authorisations. The use, retention and disposal of this information is also governed by the Safeguarding Policy.

The Information Management team can be contacted on extension 1661 or extension 3871.

The documents contained in the centrally held register should be retained for at least three years from the ending of the authorisation or for the period stipulated by the Council's document

retention policy, whichever is greater. The centrally held register should contain the following information:

- if refused, that the application was not authorised and a brief explanation of the reason why. The refused application should be retained as part of the Central Record of Authorisation.
- if granted, the type of authorisation and the date the authorisation was given and approved by the JP.
- name and rank/grade of the authorising officer.
- the unique reference number (URN) of the investigation or operation.
- the title of the investigation or operation, including a brief description and names of subjects, if known.
- whether the urgency provisions were used, and if so why.
- frequency and the result of each review of the authorisation.
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date approved by the JP.
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice.
- the date the authorisation was cancelled.
- authorisations by an Authorising Officer in urgent cases where they are directly involved in the investigation or operation (see Authorising Officer Responsibility page 17.) If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.
- the date and time when any instruction was given by the Authorising Officer.

As well as the Central Record the Information Management Team will also retain:

each application, review, renewal and cancellation, copy of the judicial application/order form, together with any supplementary documentation of the approval given by the Authorising Officer

- a record of the period over which the surveillance has taken place;

For CHIS applications

In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

- the original authorisation form, copy of the judicial application/order form, together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- the original renewal of an authorisation, copy of the judicial application/order form, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation.
- the date and time when any instruction was given by the Authorising Officer to cease using a source.

The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

Annual report to Investigatory Powers Commissioner's Office

The Council is required to provide statistics to the IPCO (was the OSC) every year in March for the purposes of the Annual Report. The Information Manager shall be responsible for completing the return and providing the statistics.

Storage and retention of material

In addition to the need to comply with the data safeguards provisions set out below, all material obtained and associated with an application will be subject of the provisions of the Criminal Procedures Investigations Act 1996 (CPIA) Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the Data Protection Act. All officers involved within this process should make themselves aware of the provisions of both the requirements under the Safeguarding Policy and the CPIA and how it impacts on the whole RIPA process.

Data safeguards

Material obtained through surveillance may include private information, legally privileged information, or other confidential material including journalistic material and constituency

business of Members of Parliament.The Council must ensure that any information it obtains through surveillance is handled in accordance with the safeguards the Council has put in place, any relevant frameworks (such as data protection), and the Home Office Codes.

Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Something is necessary for the authorized purposes where the material:

a) is (or is likely to become) necessary for the surveillance purposes set out in the legislation

b) is necessary for facilitating the carrying out of the functions of the Council under the surveillance legislation

c) is necessary for facilitating the carrying out of any functions of the Commissioner or Investigatory Powers Tribunal

d) is necessary for the purposes of legal proceedings

e) is necessary for the performance of the functions of any person by or under any enactment.

Evidence

When information obtained under a surveillance authorisation is used evidentially, the Council should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements

Reviews

As set in this document and within the Home Office Codes, regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct. Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained.

Dissemination of information

The Council will likely need to share information obtained through surveillance within the Council and between the Council and other public bodies where legally necessary. This must be limited to the minimum necessary. If a summary of the information will be sufficient to meet necessity, no more than that should be disclosed.

When sharing this type of information the Council will ensure that it has appropriate safeguards and agreements in place to ensure compliance.

Copying

Information and material obtained through surveillance must only be copied to the extent necessary. Copying includes direct copies as well as summaries and extracts.

Storage

All information and material obtained through surveillance and all copies, extracts or summaries must be stored securely to minimise the risk of theft or loss. Only those with appropriate legal authority and security clearance should be able to access the information. The Council will ensure that it has in place:

a) physical security to protect premises where the information is stored or can be accessed

b) IT security to minimise risk around unauthorised access to IT systems

Destruction

Information obtained through surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s). If such information is retained, it should be reviewed at appropriate intervals, and at least every six months, to confirm that the justification for its retention is still valid.

Confidential or privileged information

Where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business ["confidential constituent information"], authorisations can only be granted by the Assistant Director of said Service.

The reasons for acquiring information of this type must be clearly documented and the specific necessity and proportionality of doing so must be carefully considered.

Material which has been identified as confidential personal or confidential constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes.

Where confidential personal or constituent information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought

from a legal adviser to the Council before any further dissemination of the material takes place.

Items subject to legal privilege

The acquisition of material subject to legal privilege is particularly sensitive and is therefore subject to additional safeguards which provide for three different circumstances where legally privileged items will or may be obtained. They are:

a) where privileged material is intentionally sought

b) where privileged material is likely to be obtained

c) where the purpose or one of the purposes is to obtain items that, if they were not generated or held with the intention of furthering a criminal purpose, would be subject to privilege

Further details and guidance about each of the above circumstances are set out in the Home Office Codes.

Covert surveillance of legal consultations

The 2010 Legal Consultations Order provides that surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations', shall be treated for the purposes of Part II of RIPA as intrusive surveillance. **As a result, such authorisations are not available to the Council.**

Lawyers' material

Where a lawyer, acting in this professional capacity, is the subject of surveillance, it is possible that a substantial proportion of any material which will or could be acquired will be subject to legal privilege. In addition to considering the applicability of the 2010 Legal Consultations Order, the Council will need to consider which of the three circumstances that apply when items subject to legal privilege will or may be obtained is relevant, and what processes should therefore be followed.

Any case involving lawyers' material should also be notified to the Commissioner during their next inspection, and any material which has been retained should be made available to the Commissioner on request.

Handling, retention, and deletion of legally privileged material

Additional arrangements apply to legally privileged items where the intention is to retain them for a purpose other than their destruction:

a) A legal adviser to the Council must be consulted and is responsible for determining whether that material is privileged;

b) Material which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege; and

c) the Investigatory Powers Commissioner must be notified of the retention of the items as soon as reasonably practicable

Training

There will be an on-going training programme for Council Officers who will need to be aware of the impact and operating procedures with regards to this legislation. The training officer will be required to retain a list of all those officers who have received training and when the training was delivered.

Authorising Officers must have received formal RIPA training before being allowed to consider applications for surveillance and CHIS.

Errors

There is now a requirement to report all covert activity that was not properly authorised to the Investigatory Powers Commissioner's Office (IPCO) in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA (see oversight section below).

Oversight

It is important that all staff involved in the RIPA application process take their responsibilities seriously. Careful management and adherence to policy and procedures will assist with maintaining oversight and reducing unnecessary errors. The policy and use of RIPA will be monitored on an on-going basis through the quarterly meetings referred to below.

Senior Responsible Officer and RIPA Co-ordinating officer

Overall oversight within the Council will fall within the responsibilities of the Senior Responsible Officer (SRO) for the Council. The Senior Responsible Officer is Claire Felton, Assistant Director

of Legal, Democratic and Procurement Services. To assist the SRO with monitoring, ensuring the policy is kept up to date, liaising with the Office of Surveillance Commissioner and organising training for staff, the Principal Solicitor has been identified as the RIPA Co-ordinating Officer. The SRO and the RIPA Co-ordinating Officer will meet on a six-monthly basis to review the RIPA activity that has taken place, consider any changes to legislation or guidance and to review the policy and processes for RIPA and the training programme. This six-month review has been agreed by the Surveillance Commissioner's Inspector as adequate oversight for our council.

Reporting to members

Quarterly returns of all surveillance activity undertaken by Council staff including joint surveillance and Directed Surveillance using the CCTV system will be compiled by the Senior Responsible Officer and the RIPA Co–ordinating Officer and reported to the Portfolio Holder for Resources in line with the current advice in the Codes of Practice. As with the above reviews, this will also be six-monthly. It will be the role of the Portfolio Holder to report to the Cabinet any issues of concern arising out of the quarterly returns. Members will also receive an annual report to keep them updated as to the levels of RIPA activity, legislative changes, staff training and any issues regarding the RIPA policy.

Scrutiny and tribunal

Scrutiny will be provided by the Investigatory Powers Commissioner's Office or IPCO (formerly provided by the Office of the Surveillance Commissioner). The Commissioner will periodically inspect the records and procedures of the Authority to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information the Office requires for the purpose of enabling them to carry out their functions.

A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. 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 period.

Complaints can be addressed to the following address:

Investigatory Powers Tribunal

PO Box 33220

London

SW1 H9ZQ

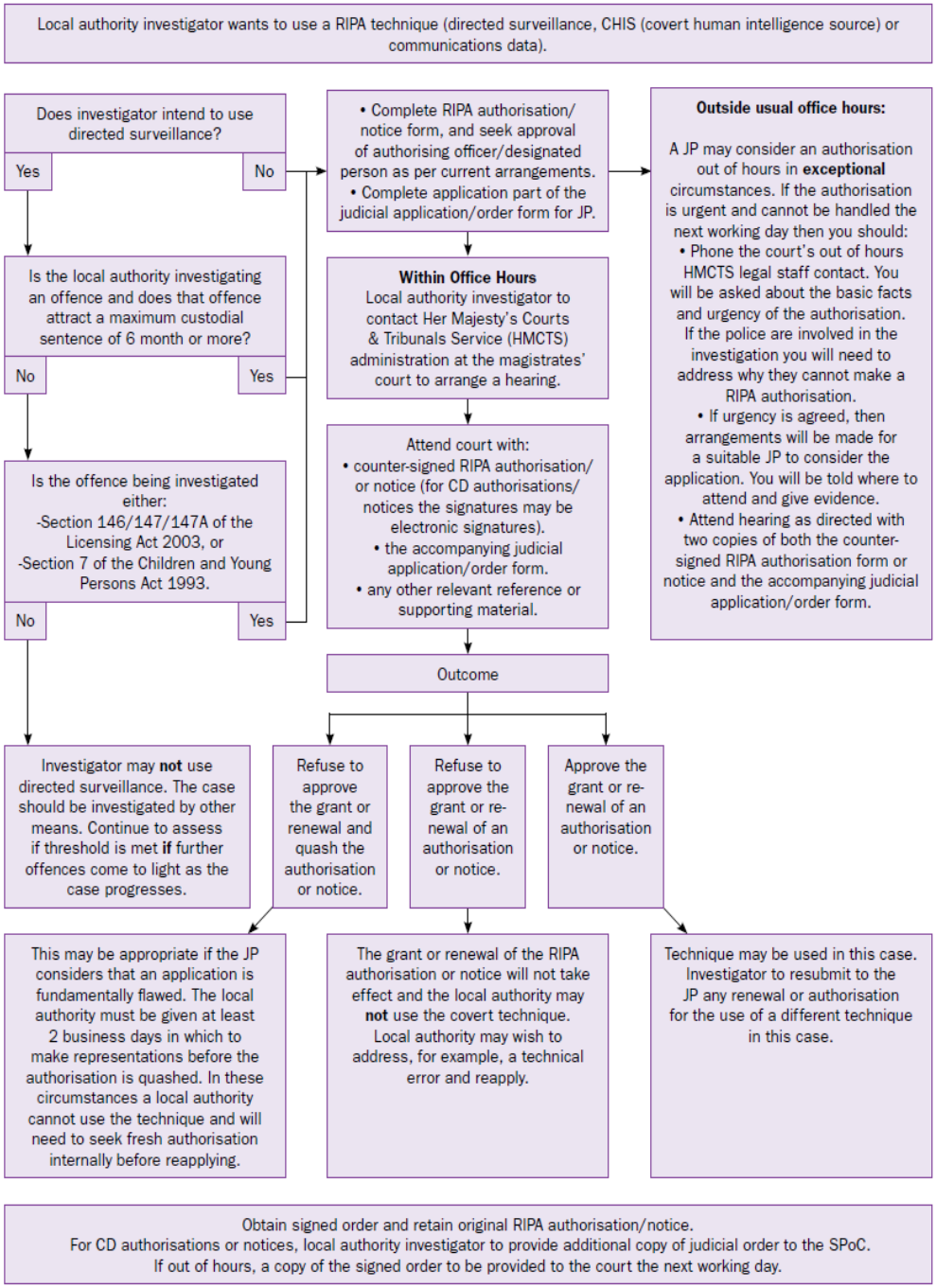
Appendix 1

List of Authorising Officers for Bromsgrove District Council and Redditch Borough Council and authorising levels:

Name	Department	Contact Number	Level of Surveillance Authority		
			Juvenile or Vulnerable CHIS and/or Confidential Material from CHIS or Directed Surveillance	CHIS	Directed Surveillance
John Leach	Chief Executive	01527 881185	Yes	Yes	Yes
Mark Cox	Director of Regulatory Services	01562 738023	No	No	Yes
James Walton	Director of Finance and Section 151 Officer	01527 64252 Ext 3055	Yes	Yes	Yes

Appendix 2

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



This chart is from the Home Office publication Protection of Freedoms Act 2012 – Changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA).