TONBRIDGE & MALLING BOROUGH COUNCIL

www.tmbc.gov.uk

Corporate Surveillance Guidance

October 2024

CORPORATE SURVEILLANCE GUIDANCE

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

CONTENTS

1. Introduction

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. RIPA regulates a number of investigative procedures, the most of recent of which is the access to communications data. This document is intended to provide officers with guidance on the use of covert surveillance, Covert Human Intelligence Sources ('Sources') and the obtaining and disclosure of communications data under RIPA. Officers must take into account any Codes of Practice issued under RIPA a copy of RIPA is available at this link: Regulation of Investigatory Powers Act 2000 (legislation.gov.uk)

The Code of Practice is available here: Covert surveillance code of practice - GOV.UK (www.gov.uk)
Regard should also be had to any guidance issued by the Investigatory Powers Commissioners' Office

All forms are available online on the Home Office website as follows: -RIPA forms - GOV.UK (www.gov.uk)

It is the policy of TMBC that use of covert surveillance, where available, is a measure of last resort to be considered only when all other avenues have been exhausted.

If you are considering the use of directed surveillance, or Covert Human Intelligence Sources please contact the Director of Central Services at the earliest possible opportunity for advice.

1.2 Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:

(a) in accordance with the law
(b) necessary (as defined in this document); and
(c) proportionate (as defined in this document)

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to

ensure both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the council could be ordered to pay compensation. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Director of Central Services.

Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This document will, therefore be kept under review by the Director of Central Services. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Director of Central Services at the earliest possible opportunity.

1.4 Scope

RIPA covers the authorisation of directed surveillance, the authorisation of sources and the authorisation of the obtaining of communications data. Communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, contents of e-mails or interaction with websites. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlap with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 2018. RIPA forms should be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

2. General

2.1 Definition of Surveillance

'Surveillance' includes:

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

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

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

Surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

2.2 Confidential Material

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The Authorising Officer shall give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authority from the Chief Executive, or, in her absence, the Director of Central Services.

3. Directed and Intrusive Surveillance

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

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

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

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

3.2 Intrusive Surveillance

That surveillance becomes intrusive if the covert surveillance:

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

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

RIPA further defines intrusive and directed surveillance as surveillance which:-

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; but

b) is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle

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

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

Where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Currently, local authorities are **not** authorised to carry out intrusive surveillance.

4. Identifying Directed Surveillance

Ask yourself the following questions:

4.1 Is the surveillance covert?

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

If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (eg in the case of most test purchases), and/or will be going about Council business openly (eg a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (eg where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that conditions are being met.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.3 Is the surveillance in such a manner that is likely to result in the obtaining of private information about a person?

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. Covert Human Intelligence Sources

5.1 Definition

A person is a source if:

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

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

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

A source may include those referred to as agents, informants and officers working undercover.

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.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or 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.

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.

This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by the Council to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (eg walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about any breaches of legislation will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

The Code of Practice states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

If there is an allegation of a noise nuisance a request to the complainant to keep a diary of times and dates that the nuisance takes place would not constitute use of a CHIS.

However, if a public volunteer was asked to obtain further information such as additional details of lifestyle, vehicle registrations etc then that person could become a CHIS.

Although an authorisation under RIPA will provide lawful authority for the use of a source it is the policy of this Council that the use of a CHIS is not permitted. If there is any doubt that there is the potential for a person to become a CHIS then guidance should be sought from the Chief Executive, Director of Central Services or the Audit & Counter-fraud Manager before any action is taken.

5A. Social Media

5A.1 Guidelines for the use of Social Media in Conducting Investigations

These Guidelines apply to all forms of social media including but not limited to Facebook, Twitter and LinkedIn:

For Facebook and Twitter, officers are to use their real name, but the account set up using their own TMBC email addresses. Personal facebook accounts must not be used.

These profiles are to be "overt" and "sterile": overt, in that there is no attempt to disguise the fact that the profile is the officer in question and identified with a TMBC email address; and sterile, in that *no content* is to be entered onto that profile. You must not make friend requests or use messaging or chat features. In twitter, you must not "follow", tweet, re-tweet or message.

All security settings must be engaged at the most secure setting.

Only information available on the public profile of a target or known associate may be accessed. No attempt must be made to access any private information such as that only viewable by "friends".

We do not consider that a single or occasional visit to a public profile or page amounts to directed surveillance. It is the electronic equivalent to a "drive past". However, officers must consider whether an operation will require continuous systematic monitoring of a profile. In this instance, a Directed Surveillance Authorisation (DSA) may be required.

Officers need to maintain awareness that a program of continuous or regular monitoring of a profile or social media account may amount to Directed Surveillance requiring a DSA. Targeted monitoring to “keep an eye” on a person of interest should be avoided. Advice should be sought at the earliest possible opportunity if there are concerns that proposed social media-based investigation might become Directed Surveillance.

In line with our existing policy, a DSA will only be considered in the event that all overt methods have been exhausted.

6. Communications Data

6.1 Definition

This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.

Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information is required from within each of the subscriber data and service use data.

a) Customer data – (Subscriber data, RIPA s21(4))

Customer data is the most basic. It is data about users of communication services.

This data includes:

- Name of subscriber
- Addresses for billing, delivery, installation
- Contact telephone number(s)
- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details
- Other services the customer subscribes to.

b) Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers

- ‘Activity’, including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- ‘Top-up’ details for prepay mobile phones – credit/debit card, voucher/e-top up details

A third type of data (traffic data) is not accessible to local authorities.

7. Management/ Authorisation Procedure

7.1 Management Structure

. The Senior Responsible Officer for RIPA compliance is Adrian Stanfield, Director of Central Services and Deputy Chief Executive. This officer is responsible for

- the integrity of the process in place within Tonbridge and Malling Borough Council to authorise directed surveillance and the use of a CHIS
- compliance with RIPA
- engagement with the Investigatory Powers Commissioner’s Office and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.
- ensuring all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Investigatory Powers Commissioner’s Office.

Day to day responsibility for RIPA compliance will fall to Joy Ukadike, Head of Legal & Democratic Services & RIPA Co-ordinating Officer. She will be responsible for

- maintenance of the Central Record of Authorisations
- collation of RIPA authorisations, reviews, renewals and cancellations
- oversight of the RIPA process/ RIPA training
- raising RIPA awareness within the Council

7.2 Authorisations

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data.

Any officer who undertakes investigations on behalf of the Council shall seek authorisation in writing for any directed surveillance or for the conduct and use of any source.

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure and procedure of which differs slightly and is outlined in paragraph 7.6.

7.3 Who can give Authorisations?

By law, the 'Authorising Officer' for local authority purposes is any Director, Head of Service, service manager or equivalent.

The use of RIPA is seen as a last resort when all other forms of investigation have been undertaken. Therefore the number of applications made by officers of this Council will be minimal. Except in cases involving juveniles, or cases which are sensitive or confidential, an authority to undertake surveillance will only be given by the Director of Central Services, Director of Finance and Transformation, Director of Planning, Housing and Environmental Health or Director of Street Scene, Leisure & Technical Services.] and should be sought from the member of Management Team responsible for the service concerned with the RIPA application.

For cases involving juveniles, or cases which are sensitive or confidential, authorisation may only be given by the Chief Executive (see 7.5.2 below).

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Director of Central Services, before Authorising Officers are certified to sign any RIPA forms. A certificate of training will be provided to the individual and a central register of all those individuals who have undergone training or a one-to-one meeting with the Director of Central Services on such matters, will be kept by the Director of Central Services.

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of any forms to the Director of Central Services, the same are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

Contact details for the Authorising Officers:

Chief Executive, Damian Roberts ext 6002

Director of Central Services, Adrian Stanfield ext 6346

Director of Finance and Transformation, Sharon Shelton ext 6092

Director of Planning, Housing and Environmental Health, Eleanor Hoyle ext 6256

Director of Street Scene, Leisure and Technical Services, Robert Styles ext 6160

7.4 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant an authorisation for the carrying out of directed surveillance, or for the use of a source or for the obtaining or disclosing of communications data unless he believes:

a) that an authorisation is <u>necessary</u> and
b) the authorised investigation is <u>proportionate</u> to what is sought to be achieved by carrying it out

For local authority investigations, authorisation is "**necessary**" in the circumstances of the particular case only if it is for the purpose of

(i) preventing or detecting crime* (Directed Surveillance);
(ii) preventing or detecting crime or preventing disorder (CHIS)

*Authorising Officers within local authorities are restricted from authorising the carrying out of Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the following additional conditions –

- the criminal offence which is sought to be prevented or detected is punishable, on summary conviction or on indictment, by a maximum term of at least 6 months imprisonment; or
- would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. These offences all relate to the sale of tobacco or alcohol to underage children.

Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe. The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities. Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved.

Collateral Intrusion

Before authorising investigative procedures, the Authorising Officer shall 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). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for an authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should immediately inform the Authorising Officer.

7.5 Approval of Magistrate

7.5.1 An internal authorisation for Directed Surveillance or the deployment of a CHIS will not take effect until such time (if any) as a Magistrate has made an order approving it. An approval is also required for the renewal of an authorisation to use either of these techniques.

The approval of a Magistrate can only be given if the Magistrate is satisfied that

a) There were reasonable grounds for the authorising officer approving the application to believe that the Directed Surveillance or deployment of a CHIS was necessary and proportionate and that there remain reasonable grounds for believing so;

b) The authorising officer was of the correct seniority within the organisation i.e. a Director, Head of Service, Service Manager or equivalent.

c) The granting of the authorisation was for the prescribed purpose i.e. preventing or detecting a criminal offence (and satisfies the Serious Offence Test for Directed Surveillance (see paragraph 7.4 above))

d) Any other conditions set out in any order under Part 2 of RIPA are satisfied (none at present).

7.5.2 In addition to the above, where the authorisation is for the deployment of a CHIS, the Magistrate must be satisfied that:

a) The provisions of section 29(5) of RIPA have been complied with. This requires the Borough Council to ensure that there are officers in place to carry out roles relating to the handling and management of the CHIS as well as the keeping of records (as per the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725)).

b) Where the CHIS is under 16 or 18 years of age, the requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) have been satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation. Note that the authorisation of such persons to act as a CHIS must come from the Chief Executive.

c) Where the application is for the renewal of a CHIS authorisation, a review has been carried out by the Borough Council and the magistrate has considered the results of the review.

It is best practice, as set out in paragraph 292 of the OSC Procedures and Guidance 2016, that the Authorising Officer should attend the Magistrates' Court to support the application and field any questions from the bench. There is no need to give notice to either the subject of the authorisation or their legal representatives.

7.6 Special Procedure for Authorisation of and Issuing of Notices in respect of Communications Data

7.6.1 The Act provides two different ways of authorising access to communications data; through an authorisation under Section 22(3) and by a notice under Section 22(4). An authorisation would allow the authority to collect or retrieve the data itself. A notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An

Authorising Officer (known as the 'Designated Person') decides whether or not an authorisation should be granted or a notice given.

7.6.2 In order to illustrate, a Section 22(3) authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

7.6.3 Applications for the obtaining and disclosure of communications data may only be made by officers of the Council. Reference should be made to the process map at Appendix 1 for guidance as to the process to be followed.

7.6.4 Notices and, where appropriate, authorisations for communications data must be channelled through single points of contact ("SPoCs") in the authority. The SPoC for Tonbridge and Malling Borough Council is James Flannery, Audit & Counter-fraud Manager. The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

7.6.5 The SPoC:

a) where appropriate, assesses whether access to the communications data is reasonably practical for the postal or telecommunications operator;

b) advises applicants and authorising officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators;

c) provides safeguards for authentication;

d) assesses the cost and resource implications to both the authorisation and postal or telecommunications operator.

7.6.6 Applications to obtain communications data should be made on the standard form and submitted in the first instance to the SpoC, and if appropriate will forward the application to the Designated Person for either the authorisation of conduct or the issuing of a notice.

7.6.7 An internal authorisation or notice to obtain communications data will not take effect until such time (if any) as a Magistrate has made an order approving it. An approval is also required for the renewal of an authorisation or notice.

The approval of a Magistrate can only be given if the Magistrate is satisfied that

a) There were reasonable grounds for the Designated Person to believe that obtaining communications data was necessary and proportionate and that there

remain reasonable grounds for believing so;

b) The Designated Person was of the correct seniority within the organisation i.e. a Director, Head of Service, Service Manager or equivalent;

c) The granting or renewal of the application was for the prescribed type of communications data to be acquired for the prescribed purpose (i.e. subscriber and service use data) to be acquired only for the purpose of preventing or detecting crime or preventing disorder);

d) Any other conditions set out in any order under Chapter 2 of Part 1 of RIPA are satisfied (none at present).

7.6.8 If approved by a Magistrate, the Designated Person will return the authorisation or notice to the SPoC who will then liaise with the postal / telecommunications company. The disclosure of data under a notice will only be made to the Designated Person or to the Council's SPoC.

7.6.9 Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 1998 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

7.7 Standard Forms

Other than urgent grants or renewals for which oral authorisations are acceptable, authorisations must be in writing.

Standard forms for seeking directed surveillance and source authorisations are available online from the Home Office website as follows: - http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/

8. Activities by other Public Authorities

8.1 The investigating officer shall make enquiries of other public authorities e.g. the police or DWP whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

9. Joint Investigations

9.1 When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (eg police, His Majesties Revenues & Customs (HMRC), The Department for Work and Pensions etc):

(a) wish to use the Borough Council's resources (eg CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain a copy of that agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

10. Duration, Renewals and Cancellation of Authorisations

10.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed.

An authorisation, once judicially approved will expire after a period of seventy-two hours, beginning with the time when the grant of the authorisation or, as the case may be, its latest renewal takes effect;

In the case of a CHIS, 12 months from the grant of authorisation

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

10.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on

the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

Standard review forms for directed surveillance are attached at Appendix 5.

10.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations. **Please note that renewals require the approval of a Magistrate (see paragraph 7.5)**.

Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired. The authorising officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired.

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance are available from the Home Office website as follows: -

http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/

10.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the authorising officer who issued it.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

Standard cancellation forms for the authorisation of directed surveillance are available from the Home Office website as follows: -

http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/

11. Records

The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the Director of Central Services. Each new application placed in the central register will be given a Unique Reference Number (URN).

In relation to communications data, the designated SPoC will retain the forms and the Director of Central Services will have access to such forms as and when required.

11.1 Central record of all Authorisations

The Director of Central Services shall hold and monitor a centrally retrievable record of all authorisations. The Authorising Officer must notify and forward to the Director of Central Services whenever a notice or authorisation is granted, renewed or cancelled to ensure that the records are regularly updated. The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These records will be retained for a period of at least three years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

11.2 Central record of Authorisations and Notices

Authorising Officers must forward details of each form to the Director of Central Services for the central record, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Director of Central Services will monitor the same and give appropriate guidance, from time to time, or amend this document as necessary. The record shall contain the following information:

a) the type of authorisation or notice
b) the date the authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the unique reference number (URN) of the investigation or operation;
e) the title of the investigation or operation, including a brief description and names of subjects, if known;
f) whether the urgency provisions were used, and if so why;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) the date the authorisation or notice was cancelled.

11.3 Records maintained in the Service

The Relevant Manager shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and a copy of the authorisation or notice together with any supplementary documentation and notification of the approval given by the authorising officer;

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

c) the frequency of reviews prescribed by the authorising officer;

d) a record of the result of each review of the authorisation or notice;

e) a copy of any renewal of an authorisation or notice, together with the supporting documentation submitted when the renewal was requested;

f) the date and time when any instruction was given by the authorising officer.

g) the unique reference number for the authorisation (URN)

Each form must have a URN. The authorising officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

12. Retention and Destruction

12.1 Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

12.2 Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

13. Consequences of ignoring RIPA

13.1 RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then **it shall be lawful for all purposes.**

Where there is interference 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 RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data 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.

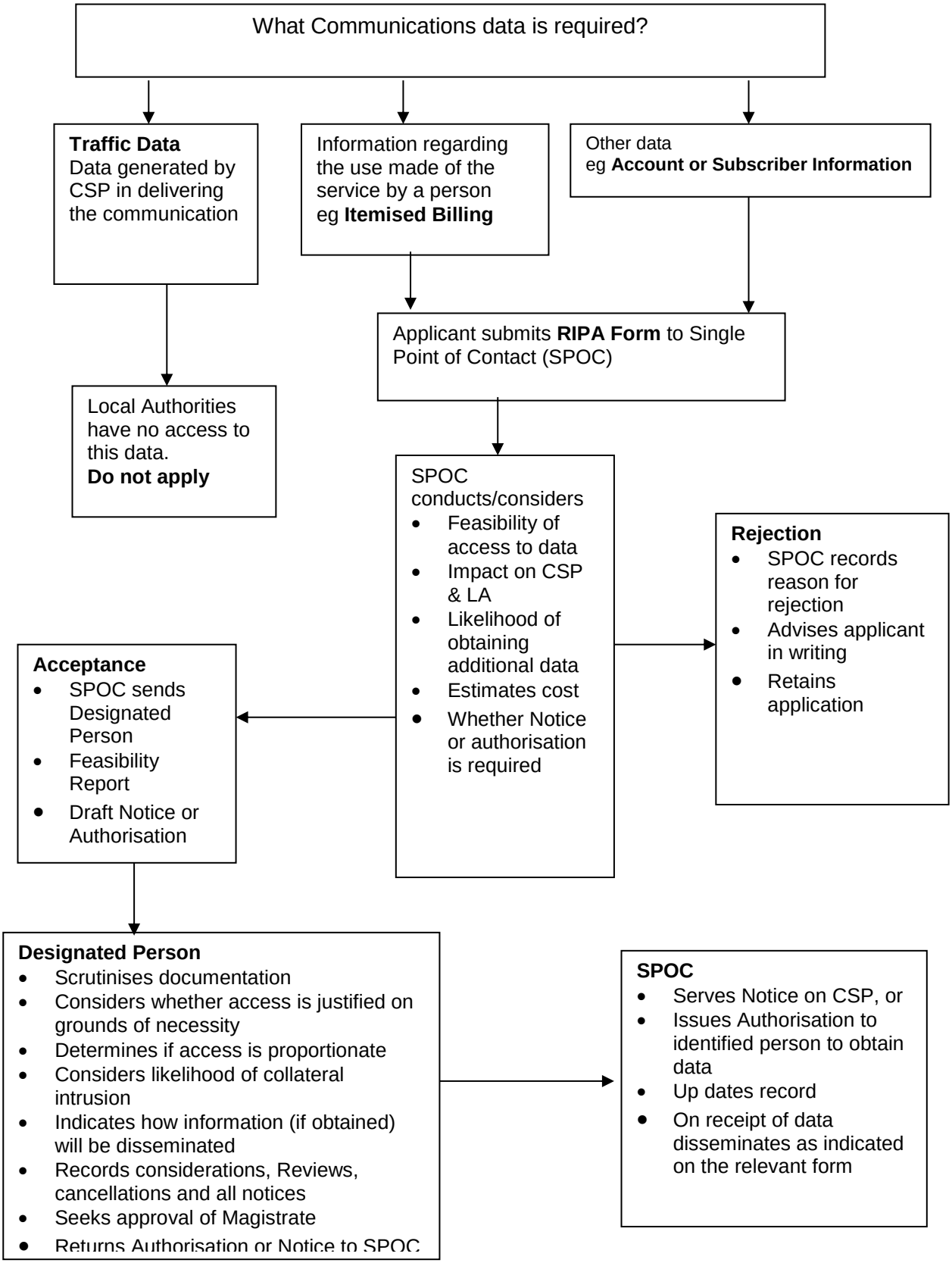
14. Scrutiny of Investigatory Bodies

14.1 The Investigatory Powers Commissioner's Office has been established under RIPA to facilitate independent scrutiny of the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at www.surveillancecommissioners.gov.uk

14.2 There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from the OSC. The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM
THE DIRECTOR OF CENTRAL SERVICES

Process Map for Accessing Communications Data



Specific Guidance to Investigators

Before authorisation for surveillance can be sought the Investigating Officer must have exhausted all possible means of obtaining the evidence that is required.

1. When the Investigating Officer feels that surveillance is the only option available they should discuss the case with the Investigation Manager. If in the opinion of the Investigation Manager surveillance is the only option left he will authorise the Investigating Officer to reconnoitre the area in which the surveillance is to take place. (The vernacular term for this is 'a drive by', but any reconnaissance must be far more thorough than simply driving past to 'have a look).

2. The fact that permission for reconnaissance has been given must be recorded on the case notes.

3. During the reconnaissance the Investigating Officer should be:

a) looking for the best vantage points to set up the observation post taking into account 'ten to two' vision of the subject, ease of following, etc.

b) making careful and detailed notes concerning Collateral Intrusion and how this can be avoided and minimised.

c) checking if material of a confidential nature may be obtained and how this can be avoided.

d) as best practice the Investigating Officer should draw a plan of the area, marking all the relevant details.

4. The Investigating Officer will then complete an Application for Directed Surveillance form.

5. This form is then to be checked by either the Chief Internal Auditor or the Investigation Manager, who will then pass the form to the relevant service Director (or Chief Executive where required) for authorisation.

6. The relevant Director (or Chief Executive where required) will apply the Surveillance Code of Practice and determine if authorisation should be given.

7. Once authorisation has been given the Co-ordinating Officer will log this fact on the Control Matrix. There after the Co-ordinating Officer will maintain the Matrix and apply the required controls.

8. A copy of the authorisation and all the accompanying paperwork will be sent, in a secure manner, to the Council's Director of Central Services. An application will then be made to the Magistrates Court for approval of the authorisation.

9. If approved by the Magistrates Court, the Director of Central Services will notify the Investigating Officer and Authorising Officer and provide a copy of the approval for their records. This will be recorded on the Control Matrix by the Co-ordinating Officer.

10. The Investigating Officer will conduct the surveillance in accordance with all legislation and codes of practice they are required to follow.

11. On starting the surveillance the Investigating Officer will make a note in their QB50 (or equivalent notebook) that they are starting surveillance. They will then keep a record of the

surveillance – they will follow the points set out in the mnemonic ADVOKATE[1] and the requirements of R v Turnbull[2]. At the end of the surveillance they will make a note in their QB50 that the surveillance has ended.

12. At the earliest opportunity the Investigating Officer will have their surveillance record signed by the Investigation Manager who will ensure the various requirements have been met.

13. The surveillance record will be kept as evidence.

14. If a renewal of the authorisation is required the Investigating Officer will discuss the matter with the Investigation Manager. If in the opinion of Investigation Manager a renewal is justified then a Renewal Application form will be completed and processed – note that the authorisation of a renewal application will also require the approval of the Magistrates Court before it comes into effect.

15. If the need for surveillance ends before the expiry date either by the Investigating Officer reporting this fact, or if this is the opinion of the Investigation Manager when reviewing the operation, then a cancellation form must be completed.

16. Once an operation has been cancelled surveillance must cease. If, for any reason, there is a need to commence surveillance again then fresh authorisation must be sought.

17. ALL details and evidence obtained must be retained in line with current legislation. Needless to say evidence that disproves an allegation must be treated with the same regard as that which does prove the allegation.

[1] **A**mount of time, **D**istance, **V**isibility, **O**bstructions, **K**nown or seen before, **A**ny reason to remember, **T**imelapse between first and subsquence description, **E**rrors betwen 1st description and actual appearance

[2] [1977] QB 224