The Regulation of Investigatory Powers Act 2000

Covert Surveillance and
Covert Human Intelligence Sources

Royal Borough of Greenwich Policy

and

procedure manual

ROYAL borough of GREENWICH

1 Introduction

This Policy and Procedure is for the carrying out of covert surveillance and use of human intelligence sources under Part II of RIPA 2000

Note:

The Investigatory Powers Act 2016, for

i. General privacy protections

ii. Unlawful Interceptions of Communications

iii. Unlawful obtaining of communications data.

Section 3 of the 2016 Act makes it an offence to intercept a communication in the course of its transmission. Upon conviction a person is liable to 2 years imprisonment or a fine or both.

Section 60A of the 2016 Act permits the Council to apply to the Investigatory Powers Commissioner, as a relevant public authority, for an authorisation to obtain communications data. It must be necessary to obtain the data for an applicable crime purpose (s.60A(8)) being:

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;

(b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.

OR,
where the Council is a party to a collaboration agreement certified by the Secretary of State.

The conduct to be authorised must be proportionate and necessary to what is sought to be achieved.

See section 73 for definition of "relevant public authorities".

Police, Crime, Sentencing and Courts Act 2022:-

Chapter 3 of the 2022 Act sets out requirements relating to the extraction of information from electronic devices, for the investigation of crime etc., and the criteria and threshold to be met, including proportionality and necessity.
The accompanying Code of Practice must be complied with.

Early consultation with Legal Services should be considered prior to any application to the Investigatory Powers Commissioner.

2 Definitions and Roles and Responsibilities

2.1 **RIPA** Regulation of Investigatory Powers Act 2000.

2.2 **The Policy** – RB Greenwich policy and procedure manual covert surveillance and human intelligence sources.

2.3 **Central Register** - Register of all RIPA authorisations cancellations and reviews

2.4 **The Senior Responsible Officer** ("SRO") - is the Director of Legal Services The SRO is responsible for:

- The integrity of the process.
- Compliance with the RIPA.
- Engagement with the Surveillance Commissioners and Inspectors.
- Overseeing the implementation of any post inspection action plans recommended by the Surveillance Commissioner.
- Ensuring that all Authorising Officers and elected Members are aware of their duties and responsibilities and that all relevant staff are appropriately trained to ensure compliance.
- Report to Overview & Scrutiny Committee.

2.5 **Members** – will review the Council's policy and consider reports on the use of RIPA (via Overview & Scrutiny Committee) periodically to ensure compliance with the Council's policy and that the policy remains fit for purpose.

2.6 **Authorising Officer** – must ensure familiarity with the relevant legislation, codes and the Council's policy and procedures. The Authorising Officer must be "Operationally Independent" from any investigation they are asked to consider for approval. If this requirement cannot be shown to have been met OR if there is any uncertainty, then a different Authorising Officer who is independent, must consider the application. It is for Authorising Officers to ensure their operational independence in each case AND their ability to demonstrate this to the IPCO (Investigatory Powers Commissioners Office) if required.

A list of the Council's Authorising Officers is at Appendix 1.

2.7 **The Magistrates Court** – The role of the Magistrates Court is set out in Section 32A RIPA. This section provides that an authorisation shall not take effect until a Magistrate has made an Order approving such an authorisation.

3 RIPA and The Human Rights Act

3.1 The Human Rights Act 1998 brought into UK law the European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 of the Convention gives everyone the right to respect for their private and family life, home and correspondence. However, it recognises that there may be circumstances in a democratic society where it is necessary for the State to interfere with this right. Any interference may only be done in accordance with the law and for clearly defined purposes.

3.2 The Council has various functions which involve observing or investigating the conduct of others. These include reducing crime and disorder, dealing with anti-social behaviour, racial harassment and noise nuisance, investigating fraud and enforcing trading standards, licensing and food safety regulations.

3.3 In most cases, Council officers carry out these functions openly and in a way which does not interfere with a person's right to privacy. But if it is necessary to use covert techniques to carry out a specific investigation, and private information about anyone is likely to be obtained as a result, RIPA authorisation is required.

3.4 The Regulation of Investigatory Powers Act 2000 (RIPA) ensures that covert techniques are used in accordance with Article 8. It provides the legal basis for council officers to authorise and use covert surveillance, informants and undercover officers whilst safeguarding the public from unnecessary invasions of their privacy. Note also the Data Protection Act 2018 and the General Data Protection Regulation which have increased the safeguards and protection of privacy and processing of private information.

3.5 This Manual sets out the Council's policies and procedures on the use of covert techniques to obtain information. All Council departments seeking to obtain evidence by using covert surveillance, or by using informants or undercover officers, must follow these procedures.

3.6 It is important to emphasise that covert techniques may only be used where they are:

- necessary in a particular case to prevent or detect crime or to prevent disorder, and
- proportionate to what is sought to be achieved by using them.

3.7 Accordingly, where the information required in a particular case can be obtained openly, covert techniques cannot be necessary and cannot therefore be used.

3.8 The government has published two Codes, Covert Surveillance and Property Interference revised Code of Practice 2018 ("the RIPA Code) and The Home Office Covert Human Intelligence Sources revised Code of Practice 2022 ("the CHIS Code"). Officers should also note the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010. The two Codes deal with:

- The purposes for which covert surveillance and covert human intelligence sources may be used
- Who can authorise their use
- What factors should be considered in deciding whether authorisation should be sought and granted
- How long authorisations last, and how they can be renewed
- What use can be made of the material gained
- What records must be kept, where and for how long
- Responsibility for compliance with the Act and the Codes
- Oversight of reporting of errors
- Implementation of post inspection action plans
- The role of elected Members

3.9 Both Codes of Practice are on the Home Office website and supplement the procedures in this Manual. The Codes are admissible as evidence in criminal and civil proceedings. If a provision of these Codes appears relevant to any court or tribunal, it must be taken into account.

3.10 Note should be taken regarding the use of juveniles as a CHIS, as provided for within the Codes of Practice and the Regulation of Investigatory Powers (Juveniles) Order 2000.

3.11 The new power to allow a CHIS to engage in crime is not available to Local Authorities.

The RIPA and CHIS codes are available on the Home Office website, www, gov.uk

Interfering with the Right to Privacy

4.1 Everyone has the right to respect for their private and family life, their home and correspondence. Covert surveillance, and using agents and undercover officers, interferes with this right. Article 8 of the Convention permits this only where the interference:

- Has a basis in law
- Is for a permitted purpose
- Is necessary
- Is proportionate, and
- Is not discriminatory

Basis in law

4.2 RIPA provides the legal basis for officers to carry out covert surveillance and to use covert human intelligence sources. The procedures in this Manual are designed to ensure compliance with RIPA, avoid legal action against the Council and make sure any evidence we obtain can be used as evidence in court proceedings.

Permitted purpose

4.3 Officers may only carry out covert surveillance and use covert human intelligence sources to prevent or detect crime or to prevent disorder and with effect from **1st** November **2012** meet the crime threshold, see paragraph 7 of the Magistrates' Courts (Regulation of Investigatory Powers) Rules 2012. Other purposes permitted by RIPA are not available to the Council.

Necessary

4.4 Covert surveillance and using covert human intelligence sources must be necessary (and not just reasonable) to achieve the prevention or detection of crime or to prevent disorder. Using covert techniques where the information could be obtained by overt methods would be unnecessary and therefore unlawful. Officers must, when applying for a RIPA authorisation, specifically state why covert surveillance is necessary as opposed to merely desirable.

Proportionate

4.5 Covert surveillance and use of covert human intelligence sources must be proportionate to what is sought to be achieved. This means RBG must use the least intrusive method. In addition, we must consider whether the use of covert surveillance in the particular circumstances is a proportionate response or measure, and whether alternative means of obtaining the information required are available. In all instances officers must consider the privacy of innocent members of the public who might be caught up in collateral intrusion. It is they who are most likely to complain and seek compensation if pictures or details of their activities and private life are misguidedly made public.

Discriminatory

4.6 Covert surveillance, and using covert human intelligence sources, must not be applied in a different way to different groups of people. Everyone has the right to privacy, regardless of their sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. Article 14 of the human rights convention must be given full effect.

5 Surveillance

5.1 Surveillance includes monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and recording anything monitored, observed or listened to. It includes intercepting post and telephone communications where the sender or recipient consents. It can be with or without the assistance of surveillance devices. It can be overt or covert.

Overt surveillance

5.2 Most surveillance carried out by the Council is overt, there is nothing secretive or hidden about it. In many cases, officers will behave in the same way as members of the public (e.g. in the case of most test purchases), and/or will go about Council business openly (e.g. a market inspector walking through markets).

5.3 Surveillance is overt even if equipment is used to reinforce normal sensory perception, such as binoculars. Routine surveillance by CCTV cameras which are visible and whose presence is signalled to the public is overt. While using other cameras could be overt, if it did not involve systematic surveillance of an individual, it would be wise to obtain RIPA authorisation if Officers go out intending to take photographs.

5.4 Surveillance will also be overt if the subject has been told it will happen. A resident might be warned that noise from their house will be recorded if the noise continues, or that their anti-social behaviour will be monitored. An entertainment license might be issued subject to conditions, and officers might visit without notice and without

identifying themselves to the owner/proprietor to check that the conditions are being met.

5.5 Overt surveillance does not require RIPA authorisation.

Covert surveillance

5.6 Covert surveillance may only be used in an investigation if the information required cannot be obtained by using overt methods.

5.7 Surveillance is covert only if it is carried out in a way that is designed to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. For example, an investigator may follow a benefit claimant from his home to his suspected workplace. Or a trading standards officer may carry a hidden camera or recording device which may obtain information about the private life of a shopkeeper.

5.8 Overt surveillance may become covert, and therefore need authorisation. For example, the controller of a CCTV system may be asked by an education officer to follow a child of school age through the town centre.

5.9 Covert surveillance requires RIPA authorisation for directed surveillance.

Directed surveillance

5.10 Directed surveillance is

- Covert surveillance, but not intrusive surveillance.
- Undertaken for the purposes of a specific investigation or a specific operation, and not by way of an immediate response to events or circumstances. For example, a trading standards officer on the way to work would not require an authorisation to conceal himself or herself and observe a market trader acting suspiciously.
- Likely to result in obtaining private information about a person, whether or not that person is specifically targeted for the purposes of the investigation or operation. 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. Family life should be treated as extending beyond the formal relationships created by marriage. In certain circumstances aspects of a person's business life may constitute private information. When in doubt consult with Legal Services.

5.11 Directed surveillance requires RIPA authorisation.

Intrusive surveillance

5.12 Intrusive surveillance is:-

- Covert surveillance
- Carried out in relation to anything taking place on residential premises or in a private vehicle. This may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance, or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside.

5.13 The Council is **not** permitted to carry out intrusive surveillance, nor to enter on or interfere with property or wireless telegraphy.

CCTV

5.14 RIPA authorisation is not generally required for the use of our CCTV systems, as the public know they exist and are a means of detecting and deterring crime. The Council has a separate Manual dealing with the use of CCTV.

5.15 Normally CCTV would not be expected to be involved in any form of covert surveillance. General CCTV operations to observe public demonstrations or to respond to immediate police requests for observation do not need to be authorised.

5.16 However, a request may be received to observe a known subject without their knowledge as part of a pre-planned operation, or to watch the outside of specific premises or to observe disruptive neighbours. These actions would be directed surveillance. If CCTV officers receive such a request, the department or organisation making the request must confirm RIPA authorisation has been obtained to ensure that the surveillance is lawful.

5.17 No directed surveillance should be undertaken by the CCTV system unless details of the serial number of the authorisation certificate have been received, along with the name of the authorising officer and the duration of the operation. All requests for directed surveillance are to be directed to the CCTV Manager (or his or her line manager) in advance of the operation. The CCTV manager or his/ her line manager must ensure that they are aware of the parameters of the surveillance authorised. CCTV operators must not authorise or take part in directed surveillance without the express permission of the CCTV Manager (or his or her line manager).

5.18 Authorising Officers from the police will normally be a Superintendent or above and they may authorise operations for up to three months. In an emergency, the surveillance request may be authorised by an Inspector but the operation may only last for seventy-two hours unless counter-authorised by a Superintendent or above.

Authorising Officers from Council departments will be Chief Officers, or the officer responsible for the management of the investigation.

5.19 The Council's CCTV system should never become involved in any intrusive surveillance operation.

6 Human Intelligence Sources

6.1 A person is a Covert Human Intelligence Source (CHIS) if he or she:

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

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

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

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

6.3 The use of a CHIS 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.

6.4 Covert surveillance against a CHIS or a potential CHIS source maybe necessary , other than those acting in the capacity of a relevant source, but must be justifiable under Article 8(2) European Convention of Human Rights.

6.5 The covert use of a human intelligence source requires RIPA authorisation.

Covert

6.6 Under 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.

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

Use

6.7 The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS. In general, therefore, an authorisation for use of a CHIS will

be necessary to authorise steps taken by a public authority in relation to a CHIS (see the CHIS Code 2010 paragraph 2.5).

The Council **cannot** authorise a CHIS to engage in crime under s.29B of RIPA 2000

Establishing, maintaining and using a relationship

6.8 The word "establishes" when applied to a relationship means "set up". It does not require, as "maintains" does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity (see the CHIS Code 2022 paragraph 2.18 and Examples 1 and 2).
Officers should, however, be aware that in some circumstances an informant even though not tasked to obtain information may be a CHIS for example where an informant gives repeat information and it becomes apparent that the informant may be obtaining that information in the course of a relationship. Such cases should be referred to Legal Services for advice. This is because in reality the informant may in fact be a CHIS to whom a duty of care is owed if the information is then to be used.

Tasking

6.9 Tasking is the assignment given to the CHIS by the person who is responsible for the general oversight of the use made of the CHIS and/or by the person who has day to day responsibility for:

- dealing with the source on behalf of the Council;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

6.10 The assignment means asking the CHIS to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the Council.

6.11 Authorisation for the use or conduct of a CHIS is required before any tasking which requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

6.12 In some instances, tasking will not require the CHIS to establish a personal or other relationship for a covert purpose. For example a CHIS may be tasked with finding out purely factual information about the layout of commercial premises. In such cases, it is for the authorising officer to determine where, and in what circumstances, such activity may require authorisation.

6.13 It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the CHIS' task. If this changes, then a new authorisation may need to be sought.

6.14 It is difficult to predict exactly what might occur each time a meeting with a source takes place, or each time the source meets the subject of an investigation. There may be occasions when unforeseen actions occur. When this happens, the occurrence must be recorded as soon as practicable after the event. If the existing authorisation is insufficient it should either be updated and re-authorised (for minor amendments only), or it should cancelled and a new authorisation obtained before any further such action is carried out.

6.15 Similarly, where it is intended to task a CHIS in a new way or significantly greater way than previously identified, officers must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This must be done in advance of any tasking, and the details of the referral must be recorded.

Juvenile sources

6.16 Special safeguards apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. **On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him**. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. In such circumstances prior consultation with the Head of Law and Governance is essential.

Collateral intrusion

6.17 The principles are essentially the same as for directed surveillance. See the CHIS Code 2022 paragraphs 3.18 to 3.21, See also *Authorisation Procedures for Directed Surveillance* above.

Confidential information

6.18 The same general considerations for covert directed surveillance and confidential information apply to the use or conduct of a CHIS and confidential information. However, the revised CHIS Code of Practice 2022 and the Covert Surveillance and Property Interference revised Code of Practice, provide guidance relating to deliberate, incidental and unintended obtaining, providing access to, or disclosure of matters subject to legal privilege.

Management responsibility

6.19 Chief Officers must ensure that arrangements are in place for the proper oversight and management of sources, including appointing the officers. The CHIS Code provides that the Council must have a Senior Responsible Officer for CHIS.

6.20 The Code provides that the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners (now IPCO). Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed (see the CHIS Code 2022). The Senior Responsible Officer is the Director of Legal Services

6.21 The officer responsible for the day-to-day contact between the Council and the CHIS will usually be of a rank or position below that of the authorising officer.

Handler

6.22 The person referred to in section 29(5)(a) of the 2000 Act (the handler) will have day to day responsibility for:

- the welfare and security of the CHIS
- monitoring, directing their activities and recording information provided.

Controller

6.23 The person referred to in section 29(5)(b) of the 2000 Act (controller) will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS (see the CHIS Code 2022).

Meetings

6.24 It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should cancelled and a new authorisation should be obtained before any further such action is carried out..

Re-tasking

6.25 Similarly where it is intended to task a CHIS in a significantly greater or different way than previously identified, the handler or controller must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded

Security and welfare

6.26 Any deployment of a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer must 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.

7 Use of Social Media

7.1 The growth of the Internet and the increasing use of social media platforms for interaction and communication is a significant source of information for gathering information and assisting with the prevention and detection of crime, changing social trends, and for engaging with the public. The new revised Code of Practice, August 2018, Covert Surveillance and Property Interference, contains a specific section on the use of social media for surveillance and gathering information. The message is that even publically available information is likely to be subject to regulation where it involves obtaining private information about an individual or a group. It does not require the seeking of an authorisation for cursory examination of social media platforms or the internet in general, however, at the point where the online searches are about to become targeted, consideration must be given to seeking an authorisation for covert surveillance. It is to be noted that a single viewing of the internet platform could also require an authorisation if it is likely to involve the recording of specific information relating to an individual or the obtaining of private information or details of lifestyle. The new revised Code of Guidance provides very helpful examples to assist investigators of scenarios that may or may not require RIPA authorisations.

Extract from Code of Practice:-

7.2 The following factors may assist in determining whether a RIPA authorisation ought to be sought:

1. Whether the investigation or research is directed towards an individual or organisation;

2. 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 of the revised Code);

3. Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

4. Whether the information obtained will be recorded and retained;

5. Whether the information is likely to provide an observer with a pattern of lifestyle;

6. Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

7. Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

8. 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.

Note 1: An internet search being conducted by a third party on behalf of the public authority is likely to require a formal authorisation.

Note 2: The directed surveillance must be necessary and proportionate to be capable of being authorised.

8 Applying for an authorisation

8.1 Authorisation must be obtained where the surveillance, or the use or conduct of a source, is likely to obtain private information from or about a person, and consequently interfere with their right to privacy. This applies whether or not that person is the subject of the investigation. Obtaining an authorisation will ensure that the surveillance, or the use or conduct of a source is carried out in accordance with the law and is subject to stringent safeguards against abuse. It is important when seeking an authorisation to provide as much information as possible and to set out clearly what precisely requires authorisation.. Where relevant attach maps or plans or other relevant documents/information.

The Regulations of Investigatory Powers (Directed Surveillance and CHIS) Order 2010 as amended, only permits a local authority to authorise the use of directed surveillance where the offence being investigated is:-

(a) punishable on summary conviction or on indictment by a maximum term of at least 6 months prison

or

(b) The offence is an offence under

(i) Sections 146, 147, or 147A of the Licensing Act 2003,

(ii) Section 7, Children and Young Persons Act 1933.

(iii) Sections 91 and 92, Children and Families Act 2014

Directed Surveillance

8.2 An application for authorisation for directed surveillance must be in writing and record:

- the reasons why the authorisation is necessary in the particular case;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of all potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and

- a subsequent record of whether authority was given or refused, by whom and the time and date.

Covert Human Intelligence Source

8.3 An application for authorisation for the use or conduct of a CHIS must be in writing and record:

- the reasons why the authorisation is necessary in the particular case;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the purpose for which the source will be tasked or deployed (e.g. in relation to a series of racially motivated incidents etc.);
- where a specific investigation or operation is involved, the nature of that investigation or operation;
- the nature of what the source will be tasked to do;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- the level of authority required (or recommended, where that is different);
- a subsequent record of whether authority was given or refused, by whom and the time and date.

9 Granting an Authorisation

[Minimum requirement:
Director, Head of Service,
Service Manager or equivalent]

Authorising Officer

9.1 Where confidential information is likely to be acquired, or where a vulnerable individual or a juvenile is to be authorised as a source, the authorising officer must be the Chief Executive or, in her absence, a Chief Officer.

9.2 In all other cases the authorising officer must be one of the officers whose details are at Appendix 1.

9.3 The authorising officer must not be responsible for authorising an investigation in which he or she is directly involved e.g. one in which he or she is to carry out the surveillance or task the source

9.4 Responsibility for authorising the carrying out of directed surveillance, or the use or conduct or a source, rests with the authorising officer and requires his or her personal authority.

9.5 When granting authorisation it is important to set out clearly what is being authorised by reference to the information provided in the request for authorisation.

Confidential information

9.6 Confidential information means matters subject to legal privilege, confidential personal information or confidential journalistic material. The Codes of Practice contain further information, and the Director of Legal Services can advise on how confidential information should be handled.

9.7 RIPA does not provide any special protection for confidential information. Nevertheless, 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. So, for example, extra care should be taken where, through the use of surveillance, it would be possible to acquire knowledge of matters which involve medical or journalistic confidentiality or legal privilege.

Vulnerable individuals

9.8 Any person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or to protect himself against significant harm or exploitation, should only be authorised to act as a source in the most exceptional circumstances.

Matters to be considered

9.9 An authorising officer may only grant an authorisation where he or she is satisfied:

- **That the authorisation is necessary in the circumstances of the particular case to prevent or detect crime or to prevent disorder.** Using covert means where the information can be obtained overtly means it would be unnecessary and therefore unlawful.

- **That the surveillance or the use or conduct of a CHIS is proportionate to what it seeks to achieve.** This involves balancing the intrusiveness of the activity on the target, and others who might be affected by it, against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case, or if the information which is sought could reasonably be obtained by other less intrusive means. The activity should be carefully managed to meet the objective in question and must not be used in an arbitrary or unfair way.

- **That the risks of collateral intrusion have been properly considered.** Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation. Those carrying out the surveillance or tasking a source must inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised, or whether a new authorisation is required.

9.10 Community Sensitivity

Any person granting or applying for an authorisation must also be aware of particular sensitivities in the local community where the surveillance is taking place, or where the source is being used. They must also be aware of similar activities being undertaken by other public authorities which could impact on the deployment of the surveillance or the source.

9.11 The authorising officer must always give authorisations in writing, including in urgent cases, and all authorisations require judicial approval by a magistrates' court.

Combined authorisations

9.12 A single authorisation may combine two or more different authorisations, but the provisions for each of them must be considered separately.

9.13 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 the Council carries out surveillance on behalf of the Benefits Agency, the Benefits Agency would obtain the authorisation and provide the Council with a copy.

Duration of authorisations

9.14 Directed Surveillance authorisations are valid for 3 months. CHIS authorisations are valid 12 months, (4 months for a juvenile) unless renewed or cancelled following a review by the Authorising Officer.

9.15 The Authorising Officer must decide, when granting an authorisation, when it will be reviewed and how often a review should take place. This should be as frequently as is considered necessary and practicable.

Review of Authorisations

Para 9.15.1 Authorising officer must review authorisation and notify the SRO in writing that the review has been completed and outcome. [*if there is no confirmation from the authorising officer, the authorisation shall be cancelled by the SRO (within 5 working days from date for review.]*

Para 9.15.2 Where the Authorisation is cancelled in default of notification by the SRO, the authorising officer and the requesting officer shall be informed in writing promptly**.**

Judicial approval

9.16 No authorisation can be given effect without approval by a Justice of the Peace in the

Magistrates Court. This is not part of the Council's procedure but a statutory requirement to ensure that RIPA authorisations are being granted appropriately following introduction of the Protection from Freedoms Act 2012.

Procedure

9.17 Once the Authorising Officer has authorised the surveillance the Council must apply to the Magistrates Court for judicial approval of the authorisation. The application to the Magistrates Court must be completed by the Authorising Officer, and submitted to Legal Services together with the authorisation. The Magistrates Court application will be completed and submitted to Court by Legal Services.

Before granting approval the Justice of the Peace (JP) must be satisfied as to the following:-

- there are reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter;
- in the case of a CHIS authorisation, that there are reasonable grounds for the local authority to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter;
- in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter'
- the local authority application has been authorised by a designated person / Authorising Officer;
- the grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:

  - 29(7)(a) (for CHIS),

  - 30(3) (for directed surveillance and CHIS):
- any other conditions that may be provided for by an order made by the Secretary of State were satisfied.

The same considerations apply where a local authority is seeking judicial approval to continue using a technique (i.e. a renewal). The JP will wish to examine whether the case still meets the principle of proportionality. In particular he or she will want to consider the content and value of the information obtained so far.

10 Review, renewal and cancellation of authorisations

Review

10.1 The Authorising Officer must carry out regular reviews of authorisations to assess whether the surveillance or the use of a source should continue, or whether the authorisation should be cancelled. The authorising officer must record the results of a review on the authorisation record and copy the review to the Head of Legal Services, who will record it on the central record of authorisations.

10.2 Where the investigation provides access to confidential information or involves collateral intrusion, authorisations must be reviewed frequently.

10.3 Where the authorisation is for the use of a CHIS the review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS .

Renewal

10.4 Before an authorising officer renews an authorisation, he or she must be satisfied that a review has been carried out.

10.5 If, before an authorisation would cease to have effect, the authorising officer considers it necessary for it to continue for the purpose for which it was given, he or she may renew it in writing for a further period of three months.

10.6 A renewal is subject to the same requirement for judicial approval as an initial authorisation. Any person who would be entitled to grant a new authorisation can renew an authorisation. An authorisation may be renewed more than once, provided it continues to meet the criteria for authorisation. The renewal should be kept and recorded as part of the authorisation record.

10.7 All applications for the renewal of an authorisation must record:

- Whether this is the first renewal, or every occasion on which the authorisation has been renewed previously;
- Any significant changes to the information provided in the application;
- The reason why it is necessary to continue with the surveillance or to use the source;

- The content, and value to the investigation or operation, of the information obtained by the surveillance or the use of the source;
- The use made of the source since the grant or latest renewal of the authorisation, and the tasks given to the source during that period;
- the results of regular reviews of the investigation or operation.

Cancellation

10.9 The Authorising Officer who granted or last renewed the authorisation must cancel it if he or she is satisfied:

- That the surveillance no longer meets the criteria upon which it was authorised;
- That the use of the CHIS no longer meets the criteria upon which it was authorised;
- That satisfactory arrangements for the CHIS' care no longer exist.

11 Records of authorisations

Records authorising directed surveillance

11.1 Records authorising directed surveillance must contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- name and grade of the Authorising Officer;
- the unique reference number of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and grade of the authorising officer;
- 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.

Records authorising the use of a source

11.2 Records authorising the use of a source must contain the following information:

- the identity of the source;
- the identity, where known, used by the source;
- any relevant investigating authority, other than the Council;
- the means by which the source is referred to within the Council and any other relevant investigating authority;
- any other significant information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the means by which the source is referred to within the Council and any other relevant investigating authority have 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;
- the date when, and the circumstances in which, the source was recruited;
- the identities of the persons who have day-to-day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare, who have general oversight of the use made of the source and who have responsibility for maintaining a record of the use made of the source;
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of the source in relation to his or her activities;

- all contacts or communications between the source and a person acting on behalf of the Council;
- the information obtained by the Council by the conduct or use of the source;
- any dissemination by the Council of information obtained in that way;
- in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer that is made or provided by or on behalf of the Council in respect of the source's activities for the benefit of the Council or any other investigating authority.

11.3 The record must be maintained in such a way as to preserve the confidentiality of the CHIS and the information provided by the CHIS .

Central record

11.4 Authorising Officers must send a record of each authorisation, review, renewal and cancellation promptly to the Director of Legal Services. The Head of Legal Services will keep a centrally retrievable record and check that each authorisation has been reviewed, renewed or cancelled. The centrally retrievable record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioners Office upon request. All records must be kept for at least three years from the ending of the authorisation.

12 Retention and destruction of the product

12.1 Where the product of surveillance or from a source could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

12.2 Attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

12.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance or use of a source from being used in other investigations. Each department must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance or the use of a CHIS. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice relating to the handling and storage of material.

13 Appendices

Appendix 1 Forms:

List of Authorising Officers

Appendix 2: Forms:

Application for Directed Surveillance Authorisation

Review of Directed Surveillance Authorisation

Cancellation of Directed Surveillance Authorisation

Renewal of Directed Surveillance Authorisation

Application for CHIS Authorisation

Review of CHIS Authorisation

Cancellation of CHIS Authorisation

Renewal of CHIS Authorisation

Application forms for Magistrates Court Approval and Guidance

Appendix 3:

Specimen Direct Surveillance Application Form

Appendix 4:

Flow Chart

Appendix 1

The following officers are designated to authorise surveillance :-

Designation	**Officer**
Chief Executive	Debbie Warren
Director of Legal Services	
Assistant Director of Finance – Governance and Audit	Brendan Costello
Head of Trading Standards	
Head of Safer Communities	Charlene Noel
Assistant Director of Community Safety and Environment	Leanna Minahan

Appendix 2

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
Name: Address: DOB: Other information as appropriate:
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

Unique Reference Number	

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).
The only ground applicable to the Council is:- For the purpose of preventing or detecting crime or of preventing disorder.
7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] *Describe precautions you will take to minimise collateral intrusion.*
9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?
10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number	

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3].

Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

Unique Reference Number	

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

Date of first review	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		Grade / Rank		
Signature		Date and time		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

Unique Reference Number	

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Name (Print)		Grade/ Rank		
Signature		Date and Time		

Urgent authorisation Expiry date:		Expiry time:	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			
Date of authorisation or last renewal			
Expiry date of authorisation or last renewal			
Review number			

1	**Review number and dates of any previous reviews.**
Review number	**Date**

2	**Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.**

3	**Detail why it is necessary to continue with the directed surveillance.**

4	**Explain how the proposed activity is still proportionate to what it seeks to achieve.**

5	**Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.**

6	**Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.**

7 Applicant's details

Name (print)		**Tel No**	
Grade		**Date**	
Signature			

8	**Review officer's comments explaining why in his/her view the directed surveillance should continue. This box must be completed.**

9	**Authorising officer's statement.**		
I, hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

10	**Date of next review**	

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			

1 Explain the reasons for the cancellation of the authorisation.

2 Explain the value of surveillance in the operation.

3 Authorising officer's statement.			
I, hereby authorise the cancellation of the directed surveillance operation detailed above.			
Name (print)		**Tel No**	
Grade		**Date**	

Signature	

4	**Time and date when the authorising officer instructed the surveillance to cease.**		
Time		**Date**	

5	**Authorisation cancelled.**		
Time		**Date**	

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			
Renewal number			

1	**Renewal numbers and dates of any previous reviews.**
Renewal number	**Date**

2	**Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.**

3	**Detail why it is necessary to continue with the directed surveillance.**

4	**Detail why the directed surveillance is still proportionate to what it seeks to achieve.**

5	Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6	Detail the results of regular reviews of the use of the investigation or operation.

7 Applicant's details			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

8	Authorising officer's comments including whether the directed surveillance should continue. This box must be completed.

9 Authorising officer's statement.			
I, hereby authorise the renewal of the directed surveillance operation detailed above. The renewal of this authorisation will last for 3 months unless further renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

Date of first review	
Date of subsequent reviews of this authorisation	

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR AUTHORISATION OF THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			

1	**Give position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.** **(Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent. Where confidential information is likely to be acquired, or where a vulnerable individual or a juvenile is to be authorised as a source, the authorising officer must be the Chief Executive or, in her absence, a Chief Officer)**

2	**The grounds on which the action is <u>necessary</u> under Section 29(3) of RIPA are:**
	For the purpose of preventing or detecting crime or of preventing disorder

3	Explain why the use or conduct of a human intelligence source is necessary in this particular case.

4	Explain why the authorised conduct or use of a source is proportionate to what it seeks to achieve.

5	Details of the purpose for which the source will be tasked or deployed.

6	Where a specific investigation or operation is involved, details of that investigation or operation.

7	The nature of what the source will be tasked to do.

8	Details of the risk assessment on the security and welfare of using the source.

9	Collateral intrusion. Indicate the potential for collateral intrusion on persons other than those targeted. Include a plan to minimise collateral intrusion.

10	Confidential information. Indicate the likelihood of acquiring any confidential information

11 Anticipated start	Date	Time

12 Applicant's details			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

13	Authorising officer's comments explaining why in his/her view the directed surveillance is necessary and proportionate. This box must be completed.

14	Authorising officer's statement.

I, hereby authorise the conduct or use of a covert human intelligence source as detailed above.

This written authorisation will cease to have effect at the end of a period of 12 months unless renewed (see separate form for renewals).

This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Name (print)		**Tel No**	
Grade		**Date**	
Signature			

Date of first review	
Date of subsequent reviews	

15	Confidential information authorisation (to be given by the Chief Executive or, in her absence, by a Chief Officer).
I, hereby authorise the directed surveillance investigation/operation as detailed above in circumstances where confidential information is likely to be acquired. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals). This authorisation will be reviewed frequently to assess the need for the authorisation to continue.	

16	Urgent authorisation. Give details of why the application is urgent.		
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

17	Authorising officer's statement. This must include why the authorising officer or the person entitled to act in their absence considered the case urgent		
Name (print)		**Tel No**	
Grade		**Date and time**	
Signature			

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

REVIEW OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			
Date of authorisation or last renewal			
Expiry date of authorisation or last renewal			
Review number			

1	**Review number and dates of any previous reviews.**
Review number	**Date**

2	**Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.**

3	Detail why it is necessary to continue using a covert human intelligence source.

4	Explain how the proposed activity is still proportionate to what it seeks to achieve.

5	Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

6	Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7	Give details of the review of the risk assessment on the security and welfare of using the source

8 Applicant's details			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

9	Review officer's comments including whether the use or conduct of the source should continue. This box must be completed.

10	Authorising officer's statement.			
I, hereby agree that use or conduct of the source detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].				
Name (print)		**Tel No**		
Grade		**Date**		
Signature				

11	Date of next review	

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

CANCELLATION OF AN AUTHORISATION FOR THE USE OR CONDUCT OF A HUMAN INTELLIGENCE SOURCE

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			

1 Explain the reasons for the cancellation of the authorisation.

2 Explain the value of the source in the operation.

3	Authorising officer's statement.		
I, hereby authorise the cancellation of the use or conduct of the source detailed above.			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

4	Time and date when the authorising officer instructed the use of the source to cease.		
Time		**Date**	

5	Authorisation cancelled.		
Time		**Date**	

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR RENEWAL OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION

Public Authority	London Borough of Greenwich Town Hall Wellington Street London SE18 6PS		
Name of Applicant		**Department/Division**	
Full address			
Contact details			
Investigation/operation name (if applicable)			
Renewal number			

1	**Renewal numbers and dates of any previous reviews.**
Renewal number	**Date**

2	**Detail any significant changes to the information as listed in the previous authorisation.**

3	**Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.**

4	**Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.**

5	Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.

6	Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

7	List the tasks given to the source during that period and the information obtained from the conduct or use of the source.

8	Detail the results of regular reviews of the use of the source.

9	Give details of the review of the risk assessment on the security and welfare of using the source

10 Applicant's details			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

11	Authorising officer's comments including whether the use or conduct of the source should continue. This box must be completed.

12	Authorising officer's statement.

I, hereby authorise the renewal of the use or conduct of the source detailed above. The renewal of this authorisation will last for 12 months unless further renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (print)		**Tel No**	
Grade		**Date**	
Signature			

Date of first review	
Date of subsequent reviews of this authorisation	

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

NAFN Court Hearing Guidance

You may already be familiar with making applications to the Magistrates for orders in connection with the investigation of offences. All courts have local practices and if the practice at your local court is different you should follow the local practice.

1. Before the hearing

Read through the authorisation and the application form for Judicial Approval thoroughly. You are welcome to amend the application form supplied by NAFN but the authorisation itself should not be amended once it has been approved by the Designated Person.

Ensure you have: **The original authorisation plus one copy.**
Two copies of the application for Judicial approval
One copy of the Court Order form.

Be prepared to explain everything to the Magistrate – remember they may never have seen an application like this before. Try and anticipate what questions the Magistrate might ask.

Check if it is necessary for your Head of Legal Services to authorise you to appear in Court.

Make sure the Court know you are coming in advance.

2. At the hearing

You should address the Magistrate as 'Sir' or 'Ma'am'. They may be accompanied by a legal adviser who will be a lawyer. The public should not be present during the application. This is important because anything heard by the public might get back to the person you are investigating.

After introducing yourself you may be asked to swear an oath (or make an affirmation). This is a matter for the Magistrate's discretion. In general it is necessary to be sworn in if what you say is going to be treated as formal evidence. If, however, what you say is a presentation about the authorisation then it is not strictly necessary for you to be sworn in. Leave this to the Magistrate. If you are asked to swear an oath you can choose to affirm

instead if you object to swearing on the Bible/Holy book. Legally there is no difference between an oath or an affirmation. It is a matter of your own personal preference/religious belief. Magistrates should be able to accommodate all religious requirements.

The Magistrate may not be familiar with RIPA. It is helpful if you offer to talk them through the application, or the entire authorisation. The Magistrate may not find this necessary but they will generally appreciate the offer.

3. If everything goes well

Ask the Magistrate to sign the order. You need to keep the original authorisation and the original signed order. The Magistrate keeps a copy of everything for the Court records. Ensure that the scanned signed application form and order are returned to NAFN.

4. If the Magistrate is not happy to approve the authorisation

In most cases it is likely that the Magistrate will be happy to approve the authorisation.

However, if the Magistrate is not happy to authorise try to get as much information as possible as to why. It might be helpful to ask them if there is any further information which can be provided in support to help persuade them in future. You cannot amend the authorisation without getting it approved again by the Designated Person, but you can amend the application for Judicial approval. You can also provide further evidence to the Magistrate outside the application – if they agree to this.

If the Magistrate considers quashing the authorisation they must adjourn the application for at least two working days to give you a chance to make further representations. Although this isn't in RIPA, it is a strict legal requirement in the Criminal Procedure Rules (rule 6.28).

Whatever the outcome you should take the original authorisation with you when you leave.

5. Need further advice

If you are not sure of what to do next or need further advice contact NAFN who will be able to assist and direct your query accordingly.

NAFN UK North NAFN UK South

Telephone: 0161 342 3727 **Telephone:** 01273 291322
Email: **spoc@nafn.scn.gov.uk** Email: **spoc@nafn.scn.gov.uk**

Appendix 3

Specimen Directed Surveillance application form

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Sample Form with Notes To Assist Completion

This form is to be completed by an officer of the local authority seeking authorisation to carry out Directed Surveillance. If granted, authorisation will last for a period of up to three months.

Code of Practice: *References to the "Code" or "Code of Practice" are to the RIPA Covert Surveillance Code of Practice.*

Unique Reference Number (URN): *This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which are issued by the same department. The idea is that, during an OSC inspection, the inspector can see which forms relate to each other. A URN also allows the form relating to each investigation to be kept together in the Central Record. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. There are no hard and fast rules.*

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			

Investigation/Operation Name (if applicable)	
Investigating Officer (if a person other than the applicant)	

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171. [1]

Insert the name and position of the Authorising Officer. This is the person who will decide whether or not Directed Surveillance should be authorised and he/she will countersign this form.

2. Describe the purpose of the specific operation or investigation.

For example:

- *To investigate acts of crime or disorder e.g. racially aggravated criminal damage and racist verbal abuse*
- *To investigate and gather evidence of a potential benefit fraud*
- *To investigate instances of illegal dumping of waste*

If possible, include the relevant legislation that would be used to prosecute offenders and/or which gives you the power/duty to investigate the matter

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

The key phrase here is "in detail." Therefore a response, which merely states, "Video camera and recording equipment will be installed at a fixed point", will not be adequate.

Your statement here needs to include what is going to be done, who is going to do it, when they are going to do it, where they are going to do it and how they are going to do it. Other points to address here include:

- *How long will the surveillance last?*
- *Specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times?*
- *Which premises are to be used and/or targeted?*
- *Which vehicles are to be used? Are they public or private?*
- *What type of equipment is to be used?*

Note that, if the Authorising Officer approves this surveillance, your authorisation will only cover you to do what you have stated here (subject to any amendments made by the Authorising Officer in box 12). Consequently you can only rely on section 27 "the RIPA Shield/Defence" only in so far as you were undertaking the activities set out in this section (as amended). Therefore it pays to include lots of detail.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

Include as much information as you have. If you do not know the identity say so. Other information could include a general description of the possible target(s).

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Your statement here should be more detailed than in Box 2. You should give details of the precise information sought by doing the surveillance. For example:

- *To ascertain what time the suspect enters and leaves the building*
- *Or to capture images of the perpetrators of anti social behaviour at (place/address)*
- *To find out who is delivering the goods to the suspect's premises etc (place/address)*

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on.(SI 2003 No.3171)*

~~*In the interests of national security;*~~

- ***For the purpose of preventing or detecting crime or of preventing disorder;***

~~*In the interests of the economic well being of the United Kingdom;*~~

~~*In the interests of public safety;*~~

~~*for the purpose of protecting public health;*~~

~~*for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;*~~

Since 5th January 2004, local authorities can only authorise Directed Surveillance for the purpose of preventing or detecting crime or of preventing disorder.

Therefore all other grounds should be deleted.

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]

State why Directed Surveillance is needed to obtain the information that is sought.

The most important question to address is – why is it necessary to use covert surveillance?

How will doing the Directed Surveillance lead to prevention or detection of crime or prevention of disorder? Factors to include

will be:

- *The offence or disorder you are investigating*
- *Seriousness of the offence*
- *Impact on victims*
- *What other means you have tried/considered to obtain the information and why are those impracticable*

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]

Describe precautions you will take to minimise collateral intrusion

When doing Directed Surveillance you may be invading the privacy of those who are not your target e.g. third parties, passers by etc. RIPA requires you to think about their rights and what you can do to minimise the impact on them of your surveillance.

Paragraph 2.6 of the Code of Practice states:

"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".

People who may be the subject of collateral intrusion include:

- *Customers or workers at a business premises*
- *Visitors to a property*
- *Friends or relatives of the suspect*

Firstly, identify here who else may be caught by the surveillance.

Secondly, state why it is unavoidable. This could be because of the nature of the premises (e.g. restaurant) or because of what the person is doing (e.g. visiting other subject/target premises) that there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.

Thirdly set out what steps you have taken to minimise collateral intrusion. This may include:

- *Using a still camera as opposed to a video camera*
- *If installing hidden cameras, only switching them on at specific times rather than all the time*
- *Narrowing the field of vision or the place where the cameras are cited*
- *Reducing the amount of surveillance done at busy times e.g. shops or places of worship*

If you cannot minimise collateral intrusion you still need to show you have considered it. You may wish to add that you cannot do anything to minimise it but you will not be making any decisions on the information gathered about third parties unless it shows them committing a criminal offence.

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 2.5]

Paragraph 2.6 of the Code of Practice states:

"This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair".

This requires you to justify the need for the surveillance and the methods used and balance those with the impact on the privacy of the subject. The DCA guide on Human Rights (page 55) states:

"When taking decisions that may affect any of the qualified rights, a public authority must interfere with the right as little as possible only going as far as is necessary to achieve the desired aim."

To demonstrate proportionality you must consider the following elements,

Is this use proposed use proportionate

- ***To the seriousness of the offence or the mischief***
- ***To the degree of intrusion on the target and other people***
- ***Have other overt means been considered and discounted***

the following issues must be addressed here

- *Can you get information using less intrusive means/other methods?*
- *What other means have you tried?*
- *What have you done to try and lessen the impact on the target? Factors to set out include:*
  - *Amount of information to be gathered during the surveillance*
  - *Impact of surveillance on the subject*

- *Timing of the surveillance*

At the same time, the above must be balanced with the need for the activity in operational terms. To demonstrate this balance you should set out:

- *What you are seeking to achieve?*
- *Seriousness of the offence*
- *Impact of the offence on the victims, others/wider community and on the public purse*

10. Confidential information. [Code paragraphs 3.1 to 3.12]

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

This is defined in the Code of Practice as communication involving confidential personal information (including health and religious counselling information), confidential journalistic material or communications subject to legal professional privilege.

Local authorities are unlikely to come across the kind of information during routine surveillance operations. However you have to be alive to the possibility and add include wording here to show how you have thought about it. For example, where you will be following someone who may end up at a church, mosque or doctor's surgery.

Note that in cases where you will be obtaining confidential information, the authorisation has to be granted by the Chief Executive or, in his/her absence, a chief officer.

11. Applicant's Details.			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

This section is for the Authorising Officer to complete. It should not be pre completed by the investigating officer. Sufficient detail must be included here to demonstrate that he/she has considered thoroughly. Reference can be made to the boxes above but "cut and paste" should be avoided.

The five "Ws" stated above must be addressed in detail. This is important so that investigating officers are clear as to what they can and cannot do and the means that they can adopt. The Authorising Officer should not be afraid to reject the application if it lacks clarify or detail.

13. Explain <u>why</u> you believe the directed surveillance is necessary. [Code paragraph 2.4] **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]**
You may refer to box 7 and 9 when completing this section. You can also add any additional factors you have considered. However, to demonstrate that you have given the issues due to thought, if it important not to cut and paste that wording or to just state "see box 7 and 9".

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 3.1 to 3.12				
This box should only be completed if you are likely to obtain Confidential Information (see box 10) through Direct Surveillance.				
Date of first review				
Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Regular reviews are stressed by the Code of Practice. Where a surveillance operation is going to last more than one month then, the Surveillance Commissioners have suggested, there should be at least a review once a month. Shorter or time limited operations may not require a review. *During a review consideration will have to be given to whether the surveillance is still necessary and proportionate. A standard form is available to record the review.*				
Name (Print)		**Grade / Rank**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

15. Urgent Authorisation [Code paragraphs 4.17 and 4.18]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

Paragraph 4.13 of the Code of Practice states:

"A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, by likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need to for an authorisation has been neglected or the urgency is of the authorising officer's own making."

In urgent cases this section still has to be completed as soon as reasonably practicable. It will be rare for a local authority to be able to claim that an authorisation was so urgent that it had to be obtained verbally.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer

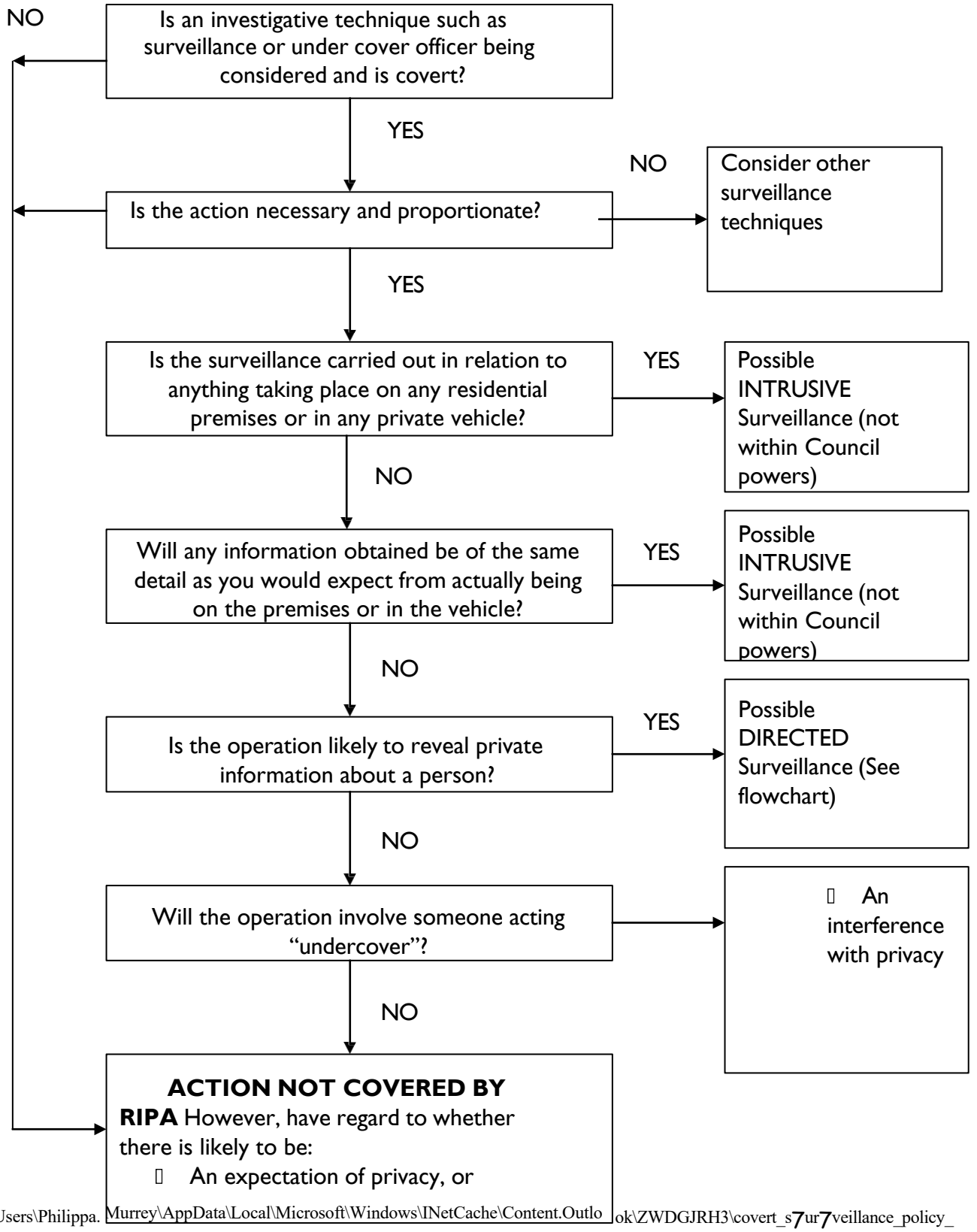
This section is only to be completed where an urgent verbal authorisation was given by an Authorising Officer only entitled to act in urgent cases. This will usually not be appropriate for local authorities.

Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

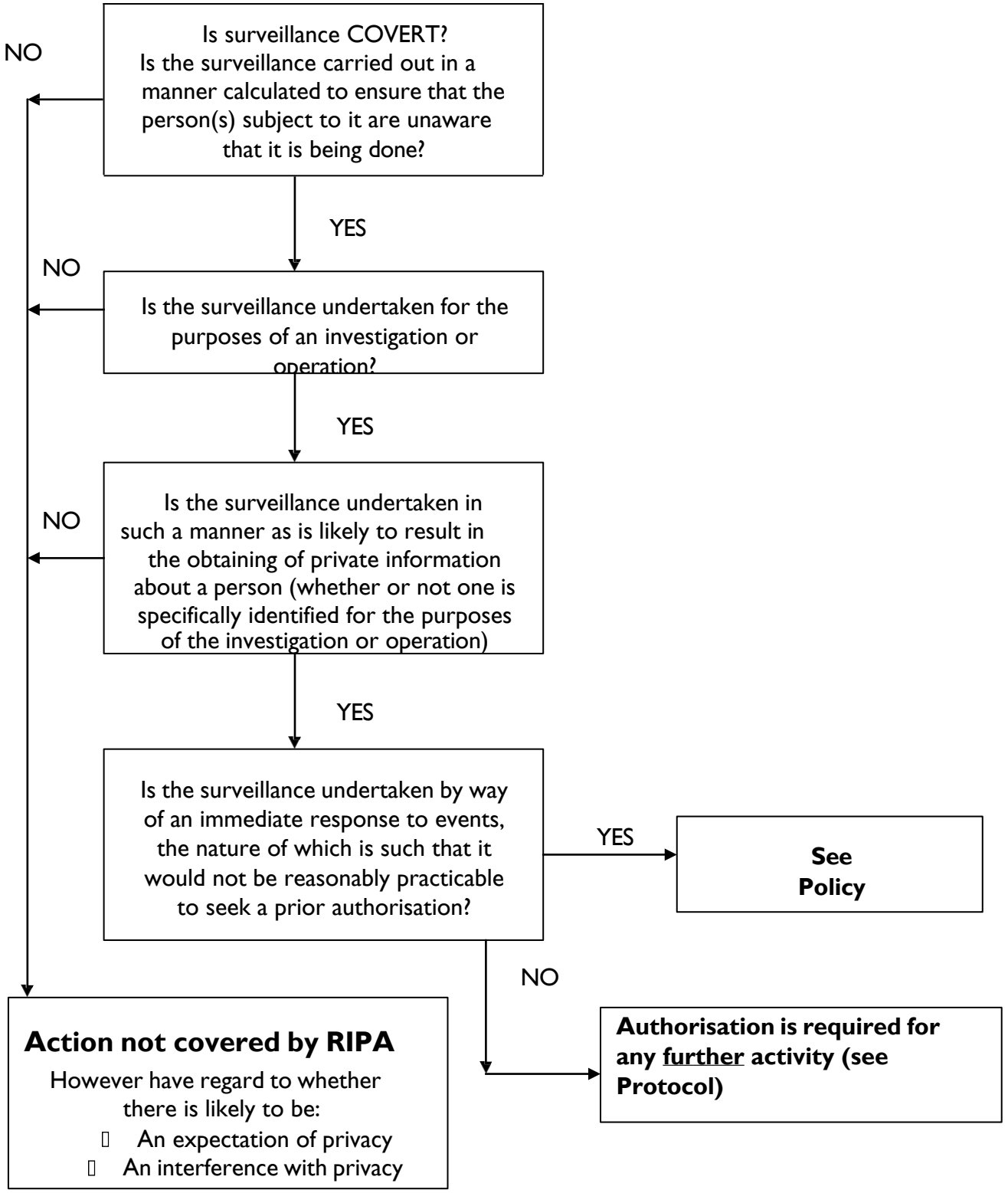
Appendix 4

TABLE 1 FLOW CHART – IS AUTHORISATION REQUIRED?

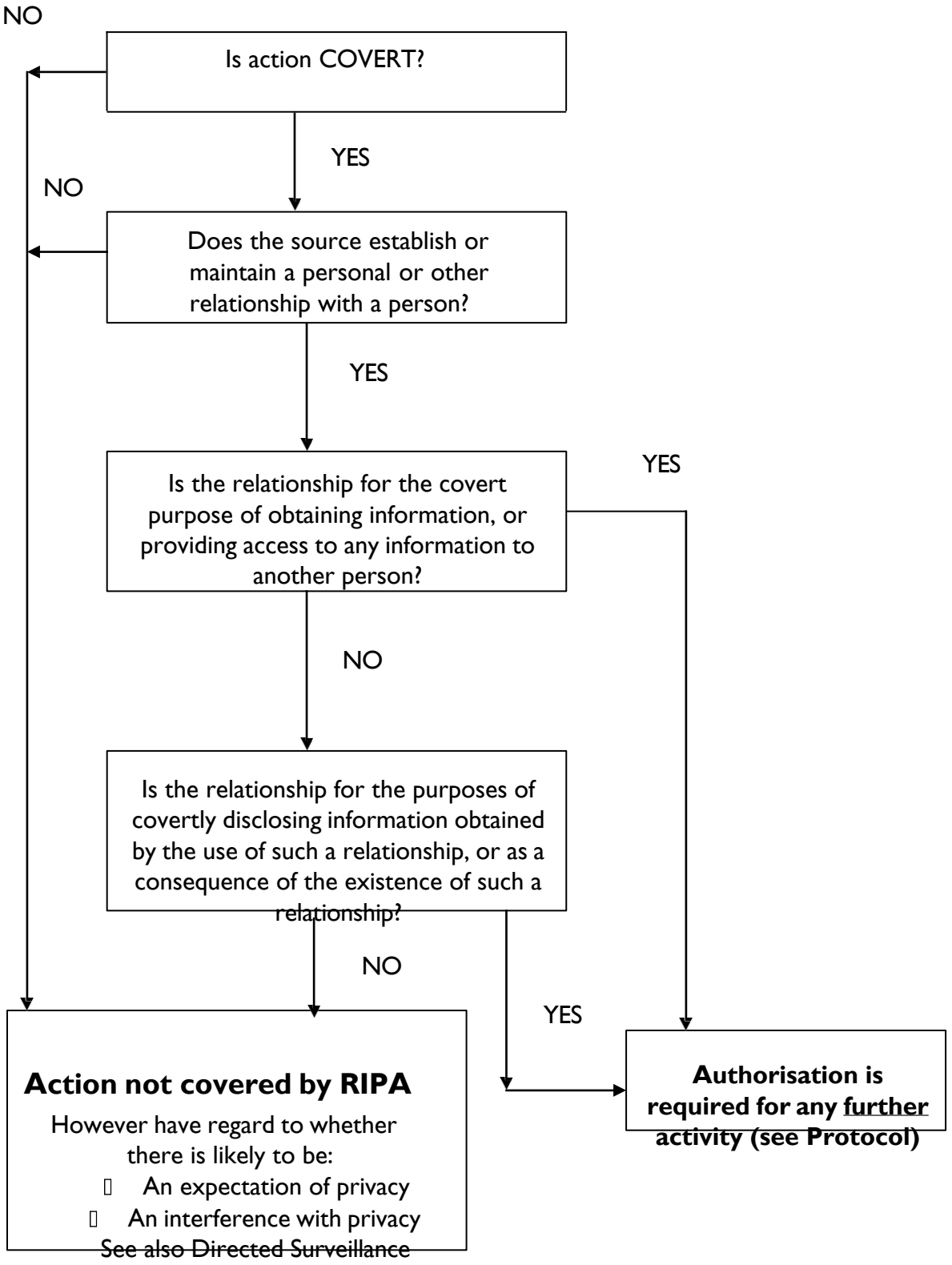


YES Possible COVERT HUMAN INTELLIGENCE SOURCE (CHIS) Surveillance
(See flowchart)

DIRECTED SURVEILLANCE



COVERT HUMAN INTELLIGENCE SOURCES



RIPA 2000 - Do you need Authorisation?