THE LONDON BOROUGH
www.bromley.gov.uk

London Borough of Bromley

Policy & Procedure on covert surveillance and the use of covert intelligence sources under the Regulation of Investigatory Powers Act 2000

Amended by the Protection of Freedoms Act 2012

Updated December 2015 incorporating recommendations from OSC Inspection on 8th October 2015
Updated November 2016 at annual review
Updated June 2019
Updated October 2022
Updated Jul 2023

CONTENTS

POLICY

PROCEDURE

LONDON BOROUGH OF BROMLEY POLICY & PROCEDURES
REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY

A INTRODUCTION

A1 The Human Rights Act requires the Council and organisations working on its behalf, to have respect for the private and family life of citizens. However, in certain cases, it may be necessary for the Council to act covertly in ways that could interfere with an individual's rights.

A2 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a mechanism for authorising covert surveillance and the use of a "covert human intelligence source" (CHIS) – e.g. undercover agents. It aims to ensure that any interference with individual's privacy is necessary and proportionate and that both the public interest and the human rights of individuals are protected.

A3 It is important to note that the legislation does not just affect directly employed Council staff. All external agencies working for Bromley Council automatically become a public body under the Act for the time they are working for the authority. It is essential, therefore, that all external agencies comply with the regulations too and that work carried out by agencies on the Council's behalf be properly authorised by one of the Council's designated authorising officers.

A4 Any officer intending to undertake covert surveillance or use a covert human intelligence source will only do so if the evidence or intelligence sought cannot be obtained by other means.

A5 If the correct procedures are not followed, evidence could be thrown out, a complaint of maladministration could be made to the Ombudsman, the Council could be the subject of an adverse report by the Investigatory Powers Commissioner' s Office (IPCO) or a claim could be made via the Ombudsman, the Courts or possibly a RIPA tribunal leading to the payment of compensation by the Council.

A6 Officers will have regard to the Covert surveillance and property interference code of practice and the Covert human intelligence sources code of practice when considering the use of covert activity.

A7 Electronic copies of all guidance relating to RIPA 20000 including copies of the Home Office Codes of Practice pursuant to section 7 of RIPA 2000 are located in the Environmental Services shared folder at EHTS/General/Phrase Library/Legal/surveillance documents/RIPA Guidance Docs.

B THE PROTECTION OF FREEDOMS ACT 2012

B1 The Protection of Freedoms Act 2012 came into force on 1 November 2012 and requires all RIPA authorisations to obtain judicial approval by a court order before they can take effect.

B2 Regulations made under the Act limits the authorisation of directed surveillance to criminal offences which carry a custodial sentence of at least six months or relate to the sale of tobacco and alcohol to children.

PROCEDURE

1 SURVEILLANCE

1.1 "Surveillance" includes:

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

1.2 Surveillance can be overt or covert.

1.3 Overt Surveillance

1.4 Most of the surveillance carried out by the Council will be overt – there will be nothing secretive, clandestine or hidden about it. 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 Bromley North market). Similarly, surveillance will be overt if the subject has been told it will happen (eg: where a noisemaker is warned 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 identifying themselves to check that the conditions are being met).

1.5 Covert Surveillance

1.6 Surveillance is covert surveillance if, and only if, carried out in a manner calculated to ensure that persons subject to the surveillance are unaware it is taking place (Section 26(9)(a) of RIPA).

1.7 RIPA regulates two types of covert surveillance – Directed Surveillance and Intrusive Surveillance and the use of Covert Human Intelligence Sources (CHIS).

1.8 Directed Surveillance

1.9 Directed surveillance is surveillance which is:

- covert surveillance;
- not intrusive surveillance (see definition below – the Council must not carry out intrusive surveillance;
- not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, eg: spotting something suspicious and continuing to observe it*)*; and
- undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). *(Section 26(10) of RIPA)*

1.10 Intrusive surveillance

1.11 Council Officers must not carry out intrusive surveillance. It is defined in section 26(3) of RIPA as covert surveillance that: is carried out in relation to anything taking place on any residential premises or in any private vehicle; and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (e.g. a listening device in a person's home or in their private vehicle).

1.12 Private Information

1.13 In relation to a person includes any information relating to his private or family life. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person may very well result in the obtaining of private information. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific operation which involves prolonged surveillance on a particular individual, authorisation may well be required. The way a person runs their business may also reveal information about his or her private life.

2 THE CRIME THRESHOLD

2.1 The Council can *only* authorise use of a directed surveillance under RIPA to prevent or detect criminal offences that are punishable by a maximum term of at least 6 months imprisonment.

2.2 The council may continue to authorise the use of directed surveillance for the purpose of preventing or detecting criminal offences under s146, 147 or 147A of the Licensing Act 2003, or s7 of the Children and Young Persons Act 1933 relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior court approval has been granted.

2.3 Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include:

- Serious criminal damage
- Dangerous waste dumping
- Serious benefit fraud

2.4 Council officers can carry out "Directed Surveillance" if, and only if, the RIPA authorisation procedures are followed.

3 EXAMPLES OF DIFFERENT TYPES OF SURVEILLANCE

Type of Surveillance	Examples
Overt	• Police Officer or Parks Warden on patrol; • Signposted Town Centre CCTV cameras (in normal use); • Recording noise coming from premises after the occupier has been warned that this may occur if the noise persists; • Most test purchases (where the officer behaves no differently from a normal member of the public)
Covert – requires a RIPA authorisation	• Officers follow an individual over the course of the day to establish whether he is working when claiming benefit; • Hidden CCTV camera focused on a railway bridge which has just been cleared of graffiti where it is expected that taggers will target the bridge • Test purchases where the officer has a hidden camera recording information which might include information about the private life of a small shop owner, eg: the way they run their business
Intrusive – Council cannot do	• Planting a listening device (bug) in a person's home or in their private motor car

4 COVERT HUMAN INTELLIGENCE SOURCE

4.1 Who is a CHIS?

4.2 A person is a CHIS if he establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.

4.3 The provisions of RIPA do not normally apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties or to contact numbers set up to receive information. However, care should be taken if the informant acquired the information in the course of, or as a result of the existences of, a personal or other relationship, where in such circumstances he is likely to be within the definition of a CHIS.

4.4 A number of different terms are used to describe those involved in CHIS operations:

4.5 Handler – means the person referred to in section 7(6)(a) of RIPA holding an office or position within the local authority and who will have day to day responsibility for:

- Dealing with the source on behalf of the local authority
- Directing the day to day activities of the source
- Recording the information supplied by the source and

- Monitoring the source's security and welfare

4.6 Controller – means the person (usually the line manager of the handler) within the local authority referred to in section 7(6)(b) of RIPA responsible for general oversight of the source. The handler and controller may not be the same person.

4.7 The conduct of a source means the actions of that source falling within RIPSA or action incidental to it i.e. what the source does.

4.8 The use of a source is any action taken to induce, ask or assist a person to engage in the conduct of a source or to obtain information by means of any action of the source

4.9 Tasking is the assignment given to the source. Either the handler or the controller may task a source. Tasking should be done only after authorisation for the use or conduct of the CHIS has been obtained. The only exception to this is where the source will not be establishing or maintaining a relationship for covert purposes, in which case authorisation may not be necessary.

4.10 Before granting a CHIS authorisation, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained. See para 7.5 of the Covert Human Intelligence Sources Code of Practice

4.11 From the above, it may be seen that both the conduct and the use of a CHIS require prior authorisation. This is effected through one application, but care must be taken to ensure that the authorisation complies with both procedures. Insurance – all applicants for authorisation must ensure that they have all the necessary insurances for an operation e.g. vehicle insurance for use of the vehicle in surveillance.

4.12 What must be authorised?

4.13 The conduct or use of a CHIS require authorisation.

- **Conduct** of a CHIS = establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information;
- **Use** of a CHIS = actions inducing, asking or assisting a person to act as a CHIS.

4.14 The Council can use a CHIS if, and only if, RIPA procedures are followed.

4.15 Juvenile Source

4.16 Special safeguards apply to the use or conduct of juvenile sources (under 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive can authorise the use of Juvenile Sources.

4.17 Where appropriate, external advice should be sought when undertaking the enhanced risk assessment for a juvenile CHIS, for example from someone with relevant professional qualifications such as a social worker or an appropriately trained health professional.

4.18 Vulnerable Individuals

4.19 A Vulnerable Individual is a person who is, or may be, in need of community care services by reason of mental or other disability, age or illness and who is, or may be, unable to take care of himself or herself or unable to protect himself or herself against significant harm or exploitation. A vulnerable individual should only be authorised to act as a source in the most exceptional circumstances. The Chief Executive is the only person who can authorise the use of a vulnerable person as a CHIS.

4.20 Test Purchases

4.21 Carrying out test purchases will not normally 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 the seller's suppliers of an illegal produce (eg: of illegally imported bush meat) is likely to require authorisation as a CHIS. Similarly, using hidden recording devices to record what is going on in the shop (eg: a hidden CCTV camera) may require authorisation as directed surveillance. A combined authorisation can be given where a CHIS is carrying out directed surveillance.

4.22 Test purchase situations and covert inspection activities are unlikely to obtain private information. However, OSC Guidance & Procedures and the Better Regulation Delivery Office guidance on Under Age sales recommend that covert test purchasing of age restricted goods, where an under-cover under age volunteer is used, the authority should apply for a directed surveillance authorisation.

4.23 Any decisions made which result in the decision not to seek an authorisation must be recorded by the investigating officer.

4.24 Noise

4.25 Persons who complain about excessive noise and are asked to keep a noise diary will not normally be a CHIS as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (eg: the decibel level) will not normally capture private information and, therefore, does not require authorisation. Recording sound with a DAT recorded on private premises could constitute intrusive surveillance unless it is done overtly – for example it will be possible to record sound if the noisemaker is warned that this may occur if the level of noise continues.

5 ON-LINE INVESTIGATIONS & SOCIAL MEDIA

5.1 Increasingly, local authorities are making use of online open and closed source intelligence opportunities when conducting investigations. The viewing of suspects Facebook accounts and other social networks is becoming a standard avenue of investigation.

5.2 The use of the internet may be required to gather evidence during the course of an investigation. This may amount to directed surveillance. Furthermore, an investigator may need to communicate with a person suspected of criminal activity by means of social media, such as Facebook.

5.3 Any use of the internet during the course of an investigation must be carefully considered with regards to Article 8 Rights of the individual, including the effect of any collateral intrusion. Where any interference with an individual's Article 8 rights is likely to be incurred, the activity should be undertaken only when necessary and proportionate to meet the objectives of the investigation.

5.4 Where private information is likely to be obtained an authorisation must be sought. Where the investigator is likely to communicate with a subject covertly, a CHIS should be considered.

5.5 . Access to open source material does not require a RIPA authorisation unless there are repeated visits to the same site.

5.6 The IPCO has expressed the view that "repeat viewing of individual open source sites for the purpose of intelligence gathering and data collection should be considered within the context of the protection that RIPA affords to such activity." Guidance can be found at para 3.10 of the Covert Surveillance and Property Interference Revised Code of Practice.

5.7 Accordingly, systematic monitoring of publicly available material may attract the need for authorisation. Where an officer accesses material that forms the essence of private life and then downloads it, stores it, retains it and processes it, then it is likely there will be an interference with Article 8 and a directed surveillance authority will be required. . Investigators should discuss with an authorising officer whether the likelihood of continued surveillance of a suspect is likely to require a directed surveillance application at the earliest opportunity.

5.8 Any use of a false identity for the purposes of a covert investigation must be the subject of an authorisation. The use of another person's photo in the course of setting up a false identity must not be considered.

5.9 A CHIS authorisation will be necessary where privacy settings are set, for example the investigator is required to become a "friend" with the suspect to facilitate a test purchase. If privacy settings are available but not applied, the data may be considered to be open source and an authorisation may not be necessary. The investigator should discuss this with the Authorising Officer on a case by case basis.

5.10 Where a decision is made not to seek an authorisation this should be recorded by the investigator and handled according to legal process.

6 APPLICATIONS FOR AUTHORISATION

6.1 Directed Surveillance and the use of a CHIS can be carried out only if authorised and only within the terms of the authorisation. Where the person applying for the authorisation is not the actual practitioner, the latter will be given a copy in order to avoid any risk of acting outside the remit of the authorisation. Appendix 1 provides a flow chart of the process from application consideration to recording of information.

6.2 Authorising Officers

6.3 Authorisations can only be given by authorising officers listed in Appendix 2.

6.4 Authorisation under RIPA is quite separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. RIPA authorisations are for 3 months and specific investigations only and must be cancelled or renewed once the specific surveillance is complete or about to expire. The duration of a juvenile CHIS authorisation is 4 months.

6.5 The Authorising Officer should not just "sign off" an authorisation but must give personal consideration to the necessity and proportionality of the proposed action and must personally ensure that the surveillance is reviewed and cancelled.

6.6 Although there is no formal guidance on who presents the application to the Magistrates, the OSC recommend that the AO should do so. Where this is not practicable, the authorisation should be presented by the applicant.

6.7 The Authorising Officer for any application should be independent to the investigation, separated from all discussions over the tactics of an investigation and any decision to make an application for RIPA authorisation.

6.8 Application Forms

6.9 Applications for authorisation should be made using standard RIPA forms. Forms seek to ensure that criteria for RIPA are fully considered.

6.10 Bromley currently uses the following modified Home Office forms:

- Application for authority for Directed Surveillance
- Cancellation of Directed Surveillance
- Review of Directed Surveillance Authority
- Application for Authority for Conduct and use of a CHIS
- Cancellation of Conduct and Use of a CHIS
- Review of Conduct and Use of a CHIS

6.11 Grounds for Authorisation

6.12 Directed Surveillance or the Conduct and Use of a CHIS can be authorised by the Council only on the grounds for the prevention or detection of crime

6.13 Assessing the Application Form

6.14 When considering whether to authorise surveillance, an Authorising Officer must:

- Consider the relevant Code of Practice
- Satisfy him/herself that the authorisation is **necessary** in the circumstances of the particular case on the grounds above, and also
- Satisfy him/herself that the surveillance is **proportionate** to what it seeks to achieve. In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer will consider other appropriate means of gathering information.
- A 2023 inspection by the Investigatory Powers Commissioners Office noted the proportionality argument presented by the applicant in a sampled application did not comply with the guidance set out by paragraph 4.7 of the Covert Surveillance and Property Interference Code of Practice (2018). The following elements of proportionality should therefore be considered: • balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm; • explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others; • considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought; • evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.
- Take into account the risk of intrusion into the privacy of persons other than the specific subject of the surveillance **collateral intrusion**. Measures must be taken wherever practicable to avoid collateral intrusion. Collateral intrusion can rarely be eliminated although in most cases it is likely to be low. The application should focus on how it can be minimised by ensuring that excessive private information is not processed as a result of the surveillance.
- Set a date for review of the authorisation
- Allocate a Universal Reference Number (URN) for the application. The URN will consist of two letters plus a number
- Ensure that the departmental log is completed and that a copy of the entry in the log is forwarded to the Monitoring Officer's Central log (Mark Bowen, Director of Legal, Democratic & Customer Services)

6.15 If there is an alternative practicable means of carrying out the surveillance which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised.

6.16 Additional Factors when Authorising a CHIS

6.17 In addition, when authorising the conduct or use of a CHIS, the authorising officer must be:

- Satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved
- Satisfied that the **appropriate arrangements** are in place for the management and oversight of the CHIS
- Consider the likely degree of intrusion of all those potentially affected
- Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained
- Ensure **records** contain statutory particulars and are not available except on a need to know basis

6.18 Urgent Authorisations

6.19 Urgent authorisations are no longer within the powers of a local authority.

6.20 Duration

6.21 The authorisation **must be cancelled** once it is no longer needed and otherwise lasts for a maximum of 3 months for Directed Surveillance and 12 months for a CHIS.

6.22 Review and Cancellation

6.23 The authorising officer must review authorisations frequently and must cancel an authorisation if he/she becomes satisfied that the surveillance is no longer required or appropriate.

6.24 The OSC consider that it would be sensible to complete the authorisation process in a form similar to other parts of the authorisation where relevant details can be retained together. When cancelling an authorisation, the Authorising Officer should:

- Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
- The reason for cancellation.
- Ensure that surveillance equipment has been removed and returned.
- Provide directions for the management of the product.
- Record the value of the surveillance and whether the objectives were met
- It is good practice that a record should be retained detailing the product obtained from the surveillance including the location of related case files and RIPA material

6.25 Cancellations must be made using the cancellation form.

6.26 Renewals

6.27 Authorisations can be renewed in writing when the maximum period 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.

6.28 The renewal will begin on the day when the authorisation would have expired.

7 RECORD MAINTENANCE

7.1 The Council must keep a detailed record of all authorisations, renewals and cancellations as set out in paragraph 8.1 of the Covert Surveillance Code of Practice, namely:

7.2 Universal Reference for Authorisations

7.3 The following Universal References relates to the authorising department:

UR	Department
ECS	Environmental & Community Services
CP	Chief Planner
ECS	Education & Care Services
RR	Recreation & Renewal
R	Director of Resources
CS	Corporate Services

7.4 Records Maintained in the Department

7.5 The following documents must be retained in the department:

- A copy of the application and a copy of the authorisation, together with any supplementary documentation and notification of the approval given by the authorising officer;
- A copy of the court application and order
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the authorising officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the authorising officer;
- The Universal Reference Number for the authorisation (URN)

7.6 Managers should promptly copy all authorisations, renewals and cancellations to the departmental unit responsible for maintaining a register of all directed surveillance and CHIS operations undertaken.

7.7 Copies of authorisations, renewals and cancellations are discoverable in legal proceedings. If proper records are not maintained, evidence gathered may be inadmissible.

7.8 Records Maintained Centrally by the Monitoring Officer

7.9 Authorising officers must forward details of each authorisation to the Director of Legal, Democratic & Customer Services for use in the maintenance of the Council's Central Register.

7.10 The Council will retain records for a period of at least three and up to five years.

7.11 The form used has been revised and expanded to contain the information set out in paragraph 8.1 of the Covert Surveillance Code of Practice as well as review dates. See Appendix 4

7.12 Oversight & review

7.13 This procedure will be reviewed annually.

Appendix 1

RIPA Authorisation Guidance Notes
(as amended following the introduction of the Freedoms Act 2012)

This document should be read in conjunction with Home Office guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance.

Applications:

1. All **new** applications (including Communication Data) and **renewal** applications must be approved by a Justice of a Peace before the surveillance or covert technique can be undertaken.

2. Only applications for offences which carry a maximum custodial sentence of 6 months or more or criminal offences relating to the underage sale of alcohol or tobacco can be made**.**

3. All directed surveillance applications are automatically authorised for 3 months (12 months for a CHIS) even though in many cases the surveillance period will be much shorter but this allows for delays in deploying equipment, not gaining evidence, etc. Authorisations for CD will be valid for 1 month from the date the JP approved the application.

    a. All authorisations **must** specify the equipment to be deployed (i.e. static camera, Mobile van) and the location where it is to be deployed and the estimated period of deployment.

    b. Within the 3 month period, **regular reviews** (i.e. monthly) should be undertaken to determine whether the surveillance should continue. This should be submitted on a **Review authorisation** form. These do not require JP approval.

4. If surveillance need not continue, the surveillance should be cancelled, and a **Cancellation authorisation** submitted. These do not require JP approval.

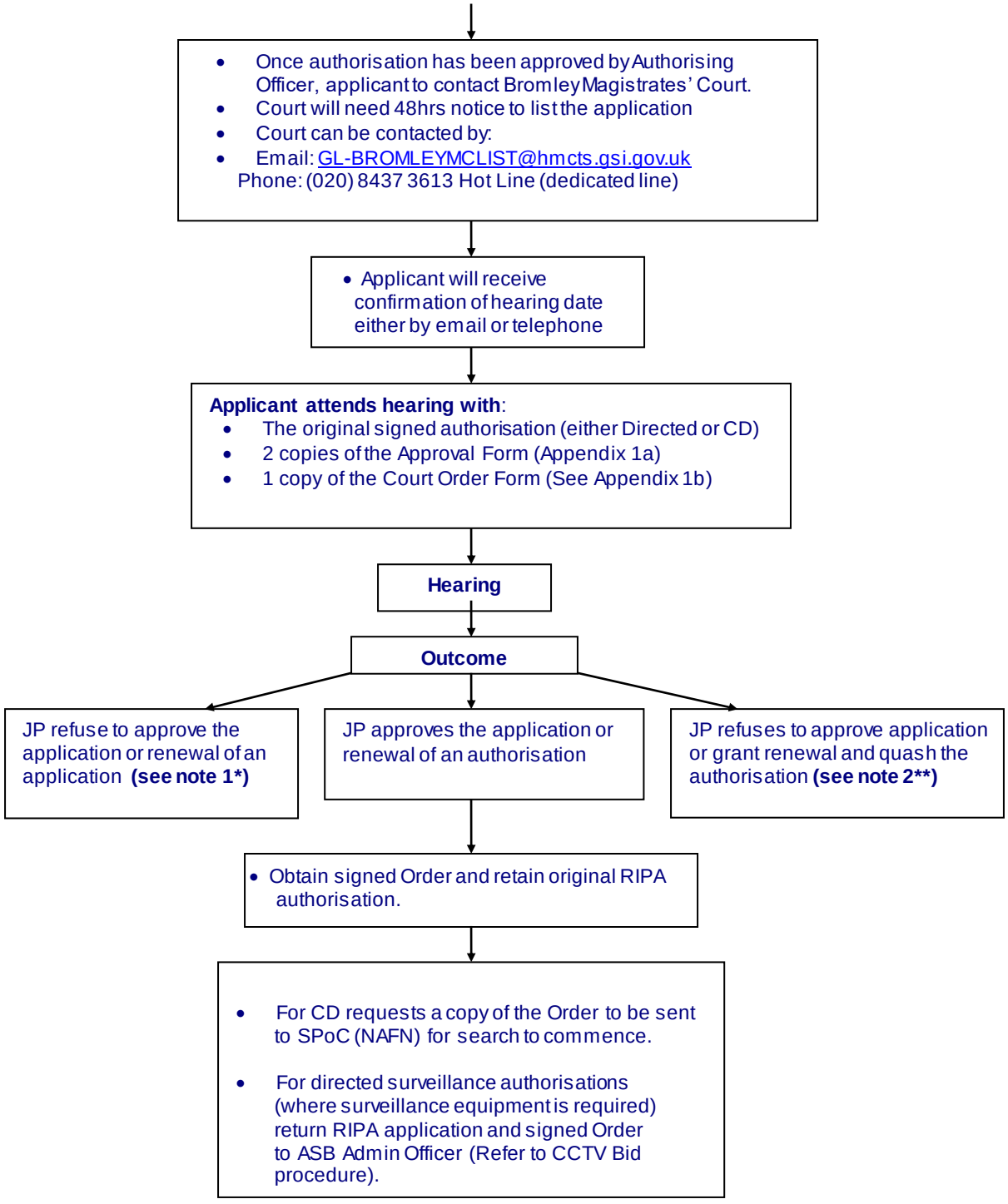
5. If before the end of the 3 months, it is deemed necessary to continue the surveillance, a **Renewal application** should be submitted. This will renew the original application for another 3 month period during which time it should be reviewed at monthly intervals. Renewal applications must be authorised by a JP. They should be made shortly before the original authorisation period is due to expire. They must be authorised prior to the expiry of the original authorisation but will run from the expiry date and time of the original authorisation.

6. All Directed Surveillance guidance and application forms can be found at:

    N:\Environmental Services\EHTS\General\Phrase.lib\legal\Surveillance Documents\New Surveillance docs

RIPA Judicial Approval Process

- For Directed Surveillance complete RIPA authorisation form and seek approval from a Designated Authorising Officer.
- For Communications Data complete online application form and submit to NAFN. (NOTE CHANGES TO AUTHORISATION RULES)
- Complete Judicial Approval Form. (Required for both Directed/CD applications (see Appendix 1a)



*Surveillance cannot take effect and applicant may wish to consider the reasons for the refusal and then reapply for approval once steps have been taken i.e. a technical error.

** This may be where the JP considers the application fundamentally flawed. At least 2 business days must be given from the date of the refusal for the applicant to make representations before the application is quashed. A new application must be submitted and authorised by a Designated Authorising Officers before reapplying.

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:……

Order made on an 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.

Magistrates' court:……

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

……

……

……

……

……

Reasons

……

……

……

……

……

……

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Appendix 2

CCTV DEPLOYMENT APPLICATION PROCEDURE
(to be read in conjunction with RIPA Authorisation Procedure Guidance Notes)

NB: No deployment will take place unless the following procedure is complied with.

1. The cctv bid form will be completed by the applicant. No direct application for deployment of equipment will be made direct to the CCTV Manager or CCTV engineer. In cases of extreme urgency applications for deployment may be made direct to a designated authorising officer/Head of Service.

2. Bid forms to be sent by e mail to ASB Coordinator who will collate all applications.

3. All police bid form applications must be authorised by an Inspector or Sergeant. A reference number relating to the RIPA must be included in the application together with a copy of the authorisation (redacted where appropriate). .

4. All bids will be assessed by the Head of Trading Standards and the ASB Coordinator. Each *deployment* will be for an initial period of 2 weeks, although the RIPA authorisation will be granted for 3 months. It will be the responsibility of the applicant and authorising officer to ensure an initial review at 2 weeks is scheduled in the RIPA application, and subsequent reviews are recorded.

5. Approved bid forms will be passed to the CCTV engineer who will visit the site and assess the most suitable equipment and location for the surveillance.

6. Following the site assessment, the CCTV engineer will inform the applicant with details of what equipment is appropriate for the deployment and details of where the equipment will be deployed.

7. On confirmation from CCTV engineer, the applicant completes a Directed Surveillance application providing full details of the deployment, including details of equipment recommended by the engineer and submits to the authorising officer.

8. For RIPA Authorisation & Judicial Approval refer to *RIPA Authorisation procedure* document. *Equipment must not be deployed until the RIPA authorisation has been approved by a JP.*

9. When deployment takes place the CCTV engineer will be responsible for recovering the equipment at the end of the agreed deployment time.

10. No Hard Drive will be issued to individual Officers. Officers will have 31 days to review their hard drives after this time the drives will be wiped clean and reissued. Any digital evidence recovered from the hard drive will be subject to internal procedures for handling digital images. Refer to *Use of Still Images Procedure.*

11. At the conclusion of the deployment the CCTV engineer will enter the result of the deployment on the CCTV master spreadsheet.

Equipment will only be issued for offences which carry a maximum custodial sentence of 6 months or more or criminal offences relating to the underage sale of alcohol or tobacco.

- Violence, hate crime, assault or abuse.
- Intimidation by acts of serious anti social behaviour involving threats
- Serious criminal damage
- There is history of continual nuisance or ASB.
- Fly tipping
- Fraud

APPENDIX 3
AUTHORISING OFFICERS

Authorising Officers must be "an Assistant Chief Officer or Investigations Manager" or above. The Authorising Officers should not be directly involved in the investigation. Only the Chief Executive can authorise the use of a vulnerable person or child as a CHIS.

Council-wide

Ade Adetosoye, Chief Executive (or, in his absence, a Chief Officer)

Only the Chief Executive can authorise:

- The use of a child under 18 or a Vulnerable Person to be a CHIS
- Operations where confidential information may be obtained. Confidential information includes matters subject to legal privilege, confidential personal information or confidential journalistic material. This includes information relating to the physical or mental health or to spiritual counselling or assistance given or to be given to a person. Legal advice should always be taken in these circumstances.

Chief Executive's

Deputy Chief Internal Auditor	Francesca Chivers

Environment & Community Services

Head of Community Safety & Domestic Regulation	Sarah Newman
Head of Commercial Regulation	Rob Vale
Assistant Director Public Protection	Louise Watkinson

Corporate Services

Director of Corporate Services	Tasnim Shawkat

Recreation & Renewal

Development Control Manager	Tim Horsman

Education & Care Services

Chief Executive	Ade Adetosoye
Director Social Care	Kim Carey

Appendix 4

Record sheet

REF NUMBER	OFFICER AUTHORITY	MAGISTRATE COURT AUTHORIITY	OFFICER INFO	OPERATION INFORMATION	URGENCY Y/N	CONFIDENTIAL INFO S.54 Y/N	AUTH BY INVOLVED OFFICER Y/N	REVIEWS DUE	RENEWED TO/OFFICER INFO	CANCELLED DATE

Appendix 5
IPCO Surveillance and CHIS Inspection of the London Borough of Bromley – February 2023

Number	Description	Evidence of correction	Date corrected
1	The 2015 recommendation highlighted that the COUNCIL'S RIPA policy did not reference the requirement for a risk assessment to be completed prior to the deployment of a CHIS.	See 4.10 and 4.17	30th June 2023
2	The SRO to ensure a process is in place to conduct regular reviews of extant directed surveillance authorisations	SharePoint system for central records is in development. 6 monthly review meetings set up for formal review of RIPA activity	SharePoint development on going First meeting 30th June 2023 Second meeting 6th November 2023
3	Future cancellations must reference the location of related case files and RIPA material	A reference to this requirement is inserted at 6.24. Advice note circulated to all staff and raised at departmental training sessions on 7th and 8th March 2023	To be reviewed on 6th November 2023
4	Central Record of authorisations must be reviewed to ensure documentation held complies with corporate record retention periods.	6 monthly review meetings set up for formal review of RIPA activity	First meeting 30th June 2023 Second meeting 6th November 2023
5	SRO to consider how they will ensure that regular record retention reviews, performed against the Central Record of authorisations and related case files, are undertaken in tandem, removing the risk that one element of each is retained for longer than the other	6 monthly review meetings set up for formal review of RIPA activity	First meeting 30th June 2023 Second meeting 6th November 2023
6	Feedback on a authorisation was that the assertion that surveillance would not result on collateral intrusion was incorrect.	The applicant in this case has been advised of the comments and an there is an insertion at 6.14	30th June 2023

7	The proportionality argument presented by the applicant did not comply with the guidance set out by para 4.7 pf the Covert Surveillance and Property Interference Code of Practice	Further detail added regrading proportionality at para 6.14	30th June 2023
8	The AO did not clearly state what he was authorising	Training covered this on 7th and 8th March 2023	8th March 2023
9	Incorrect expiry date making it unclear from the details provided when the cameras had been deployed.	This has been raised with applicants and AOs for future applications	30th June 2023
10	Delivery refresher training to all staff	Completed across two days, attended by 30 officers	7th and 8th March 2023
11	Replace ref to Office of Surveillance Commissioner by IPCO in this document	Completed	30th June 2023
12	The wording at 5.5 is confused and thus ambiguous and requires re-drafting	Note changes at 5.5 and 5.6	30th June 2023
13	Para 6.4 should include the duration of juvenile CHIS authorisations as 4 months	Note changes at 6.4	30th June 2023
14	In para 6.28 the reference to urgent renewals is incorrect and should be removed	This has been removed	30th June 2023
15	Guidance on the use of social media and internet for surveillance purposes however it is suggested that this section be reviewed actively following the delivery of the planned RIPA training to ensure it accurately summarises current practices	We asked the trainer to focus on the use of social media which included a number of scenarios encouraging officers to identify when thresholds were met, and RIPA applied. A reference to guidance has been inserted at 5.6	30th June 2023