22/23 Annual Counter Fraud Report

Appendix F

Regulation of Investigatory Powers Act 2000 Corporate Authorisation Policy

June 2023

Regulation of Investigatory Powers Act 2000
Corporate Authorisation Policy

APPENDIX LIST (documents attached within PDF)

Appendix 1 – List of Camden's Authorising Officers/Approved Rank Officers

Appendix 2 – Application for Authority for Directed Surveillance

Appendix 3 – Review of Directed Surveillance form

Appendix 4 – Application for Renewal of Directed Surveillance Authority Form

Appendix 5 – Cancellation of Directed Surveillance Form

Appendix 6 – Application for Authorisation of the Use or Conduct of a CHIS

Appendix 7 – Review of the Use of a CHIS form

Appendix 8 – Application for Renewal of the Use or Conduct of a CHIS

Appendix 9 – Cancellation of the Use or Conduct of the CHIS

Appendix 10 – General Application for Authority for Directed Surveillance

Appendix 11 – General Review of Directed Surveillance Form

Appendix 12 – General Application for Renewal of Directed Surveillance Authority Form

Appendix 13 – General Cancellation of Directed Surveillance Form

Appendix 14 – General Application for Authorisation of the Use or Conduct of a CHIS

Appendix 15 – General Review of the Use of a CHIS Form

Appendix 16 – General Application for Renewal of the Use or Conduct of a CHIS

Appendix 17 – General Cancellation of the Use or Conduct of the CHIS

Appendix 18 – LACORS Test Purchases Guide

Appendix 19 – Application to Magistrate for RIPA Approval

Appendix 20 – Local Authority procedure for the Judicial Review Process

Appendix 21 – Flowchart showing the Authorisation Procedure

INTRODUCTION

This procedure ensures that any surveillance carried out or requests for communications data by Camden officers meets the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) (as amended), the Regulation of Investigatory Powers (Communications Data) Order 2010, the Human Rights Act 1998, the Protection of Freedoms Act 2012 and the Investigatory Powers Act 2016 (IPA).

Any consideration of an application for the use of a power under RIPA should be discussed with the RIPA Senior Responsible Officer (SRO) and/or RIPA Co-ordinating Officer before an application is commenced.

All investigations that involve surveillance or requests for information relating to communications data are open to inspection and scrutiny by the Investigatory Powers Commissioner's Office (IPCO) and are subject to review on a minimum triennial basis. Prior to September 2017, this function was carried out by the Office of Surveillance Commissioners (OSC) and the Interception of Communications Commissioner's Office (IOCCO). Reviews will highlight inconsistencies and any necessary improvements needed to comply with the legislation. It is essential, therefore, that all surveillance is appropriately authorised in accordance with this procedure.

This document deals with the procedures that all Camden officers (or its agents) are required to follow when involved in the acquisition of communications data or a covert surveillance operation. These are based on the Home Office Code of Practice which can be accessed via the link below:

Covert Surveillance and Property Interference – Revised Code of Practice – August 2018

In addition, the Home Office Codes of Practice in relation to the Acquisition and Disclosure of Communications Data and Use of Covert Human Intelligence Source (CHIS) can be accessed via the links below:

Communications Data – Code of Practice – November 2018

Covert Human Intelligence Sources – Revised Code of Practice – December 2022

If you have any questions on this procedure or surveillance in general please contact the RIPA SRO (Head of Internal Audit, Investigations and Risk Management) or the Head of Legal Services for advice. The Council has designated the role of RIPA Co-ordinating Officer to the Internal Audit Investigations & Risk Management (IAIRM) Service, who will be responsible for maintaining the Council's central filing system as required by the Act. The Council has one fully trained RIPA Co-ordinating Officer to answer any queries relating to RIPA. A flow chart showing the judicial review application process and the authorisation procedure can be found at Appendix 20 and Appendix 21.

PART 1 – DIRECTED SURVEILLANCE

All IOs and AOs must also refer to the Covert Surveillance and Property Interference – Revised Code of Practice for examples and guidance when completing an application.

1.1 What is surveillance?

Surveillance can involve monitoring, observing or listening to people. This includes their movements, conversations, activities or other communications or recording anything with a surveillance device.

Overt surveillance takes place where the surveillance is not hidden, such as alerting the public to the use of CCTV in a public place. Overt surveillance **does not** require authorisation.

Covert surveillance is where the person or people under observation are not aware that surveillance is taking place.

Directed surveillance is covert in nature but is not intrusive, this means that it does not involve entry or surveillance inside a private residence or vehicle. All directed surveillance carried out by Camden officers must be authorised.

Intrusive surveillance is that which is carried out with or without a device in relation to anything taking place on any residential premises or in a private vehicle and involves the presence of an individual or device.

NB - Camden officers can only be authorised to conduct intrusive surveillance if they are involved in surveillance with other enforcement agencies (e.g. Police, Customs & Excise, etc.) in which case the authorisation would be obtained by the other agency.

In cases of surveillance on members of the public, it is clear that the Council is acting as a public authority. This means that the Human Rights Act and RIPA clearly apply. In cases where an employee is under investigation, the Council's role is that of an employer and not a public authority. RIPA does not apply in these cases. However, it is likely that any tribunal hearing cases involving surveillance will consider the human rights issues when making decisions. Furthermore, if the employee is under investigation for a criminal offence, the Council must comply with RIPA if the surveillance evidence is to be admissible.

Covert surveillance can only be justified where other investigation methods would not obtain the necessary evidence.

Who is authorised to conduct surveillance?

The Council's legal powers to conduct surveillance derive from s.111 of the Local Government Act 1972 as being ancillary to its powers to prosecute under s.222, or other legislation such as the Environmental Protection Act 1990 and Enterprise Act 2002. There may also be powers under the Local Government Act 2000 in connection with the power to promote economic well-being. Officers of the Council have the power to conduct surveillance in pursuance of their normal operational functions. ***However, they would***

need to ensure that any such action had been properly authorised as laid out in this document.

A statutory code entitled *'The Code of Practice on the Use of Surveillance'* came into force on 1 August 2002. The Council has adopted this code and it should be complied with when conducting surveillance. A revised *Covert Surveillance and Property Interference Code of Practice* came into effect from August 2018. All Investigations Officers (IO) and Authorising Officers (AO) must reference this Code when completing an application.

The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisations subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorisation from a judicial authority, before it can take effect. In England and Wales an application for such an Order must be made to a Justice of the Peace (JP). If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he or she will issue an order approving the grant or renewal for the use of the technique as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

Applications for communications data no longer require approval by a JP at a Magistrates' Court. These applications are now approved by the Office for Communications Data Authorisations (OCDA).

Those matters which fall within the criminal investigation remit are clearly governed by the procedures within RIPA and the Code of Practice. Where investigations are being pursued with a view to non-criminal proceedings, the spirit of this legislation and the code will be applied. This means that the authorisation, renewal and cancellation procedures detailed below should be followed for all types of surveillance activity. The standard Home Office RIPA forms that have been adapted for Camden Council are to be utilised for criminal investigations. A second set of forms has been designed for non-criminal investigations. Both sets can be found in the Appendices to this procedure.

All contractors or agents of the Council when acting on behalf of the Council fall within the scope of RIPA and for the purposes of the work they do for the Council are considered a public body. Therefore, proper authorisation procedures must be followed prior to any surveillance being conducted by them.

Collaborative Working

- Applicants should always consult with senior Police in their area to ensure no duplication or potential impingement on their work.
- Where there is a multi-agency operation, the "Tasking Agency" or Lead Authority should obtain the authorisation, clearly detailing the scope and other agencies involved.
- One application per operation.
- Where an individual or a non-governmental organisation is acting under direction of a public authority then they are acting as an agent of that public authority and any activities they conduct which meet the 2000 Act definitions of directed or intrusive surveillance or amounts to property interference for the purposes of the

Intelligence Services Act 1994 or the Police Act 1997, should be considered for authorisation under those Acts.

1.2 Seeking authorisation

In all instances, Investigating Officers should contact the RIPA Co-ordinating Officer to obtain a Unique Reference Number (URN) at the start of the application process. This URN must be written on the form.

If an Investigating Officer (IO) considers it necessary to undertake surveillance as part of an investigation, s/he must complete an Application for Authority for Directed Surveillance Form, see *Appendix 2*.

The form must record why the IO considers surveillance **necessary** and **proportionate** to what is hoped to be achieved. When considering an application, officers need to be aware of the following requirements:

Necessity – covert surveillance shall only be undertaken where it is designed to achieve a legitimate objective. The only reasons for which directed surveillance may be necessary to be carried out by the Council under this legislation are:

- preventing or detecting crime
- prevention of disorder

NB. It must be necessary in that particular case

Proportionality – the use and extent of covert surveillance shall not be excessive, i.e., it shall be in proportion to the significance of the matter being investigated. It must be specific and not designed to cover a wide range of situations. The officer shall make an assessment of the duration of the surveillance or each stage of the surveillance and the resources to be applied.

Collateral intrusion – reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out. The officer shall also consider how any third party information obtained will be handled. The IO should record any collateral intrusion that might occur. Collateral intrusion occurs when individuals who are not part of the surveillance are unintentionally included in the course of the surveillance. For example, where photographing a target at a specific location the inclusion of members of the public in photographs may be unavoidable.

Subsidiarity – the surveillance must cause no greater invasion of the right to privacy and is absolutely necessary to achieve its objective. All other means must be considered prior to surveillance being deemed necessary.

Minimum indictable offence – the new condition set out in article 7A(3)(a) or (b) is that the **criminal offence** which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term **of at least 6 months of imprisonment**, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

The 2012 Order also removes the previous second limb of **s.28(3)(b)** – preventing disorder.

A six-month imprisonment test will prevent Directed Surveillance being used for minor offences such as dog fouling or littering but there is an exception to the general rule in that the seriousness test does not apply to underage sales of alcohol and tobacco.

1.3 Role of the Authorising Officer (AO)

AOs must ensure that they are satisfied that the case for the proposed surveillance by the IO is necessary and proportionate.

AOs may not approve Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the condition set out in the new article 7A(3)(a) or (b) of the 2010 Order [Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010/521], which prescribes which officers in a public authority have the power to grant authorisations for Directed Surveillance.

An AO should consider all information provided on the Application for Authority for Directed Surveillance and if necessary, ask for further information from the IO. When completing the form the AO should write down exactly what they are authorising. All authorities must be signed, showing the date and time the authority was granted.

The AO should return the completed form to the IO who should keep a copy on the investigation file and forward the original marked '*private and confidential*' to the RIPA Co-ordinating Officer for filing on the central file.

1.4 Officers designated to grant authority

There are three levels of designated authority:

Responsible Officer	**What is being authorised**
Head of Paid Service (Chief Executive)	Children/Vulnerable Adults or where confidential information is likely to be obtained.
Executive Directors and Directors	All other authorisations including CHIS

Surveillance may only be authorised by officer of third tier level or above. In the absence of a nominated AO the authorisation must be given at a more senior level. The AO need not necessarily work in the same area of business activity.

Only nominated and trained AOs are permitted to grant authorisations, as per this policy. The Head of Internal Audit & Investigations maintains a list of officers approved to undertake the role of an AO this is attached at *Appendix 1*.

NB. AOs should not be responsible for authorising surveillance for an investigation in which they are directly involved. Any unavoidable incidents of "self-

authorisations" will be recorded on the Central Record and be brought to the attention of IPCO at its next inspection.

1.5 Training

The role of an AO carries great responsibilities for themselves, as well as the staff involved in the surveillance operation, the Council and members of the public. In order to protect the Council from the risk of misuse of the powers under the Act, no one will be permitted to carry out the role of an AO or undertake duties under RIPA as an applicant, RIPA Co-ordinating Officer or Gatekeeper without having first undergone approved training. All AOs and relevant staff will be expected to undertake refresher training. The Head of Internal Audit & Investigations should be contacted for further information**.**

1.6 Length of authorisation

A written authorisation will last for not more than three months, less one day, unless cancelled or renewed.

In all cases regular reviews should be carried out and a renewal or cancellation must be undertaken no more than three months from the date of the original authorisation.

1.7 Surveillance Equipment – Control/Inventory

It is the responsibility of the Service Head to ensure the issue and use of any equipment held by the service for the purpose of conducting covert directed surveillance (e.g. radios, cameras, etc.) is correctly recorded and usage is subject to audit.

1.8 Reviews

The AO should ensure that they review the authorisation at least monthly in order to satisfy themselves that authority should continue. Evidence of this review should be completed on the Review of Directed Surveillance Form, see *Appendix 3*.

1.9 Renewals

There may be circumstances where the investigation requires surveillance to take place for a period longer than three months. In such cases, it will be necessary for the IO to obtain a renewal of authority from the AO and, in common with an initial authorisation, it will also need to be approved by a magistrate. A copy of the Application to Magistrate for RIPA Form is available at *Appendix 19*.

The IO should submit a renewal form with a copy of the original Application for Authority for Directed Surveillance to the AO. A copy of the Application for Renewal of Directed Surveillance Authority Form, is available at *Appendix 4*.

The AO must review both documents to ensure that there is continuing justification for surveillance. A copy of the renewal and the magistrates' approval forms should be placed on the investigation file and the original sent marked 'private and confidential' to the RIPA Co-ordinating Officer to place on the central file.

1.10 Cancellations

Surveillance should be no longer than necessary to gather the required information. The AO must cancel the authorisation if satisfied that the directed surveillance is no longer required by completing a Cancellation of Directed Surveillance Form, see *Appendix 5*.

The AO must make reference on the cancellation form to the handling, storage and destruction of any material obtained from the directed surveillance. The AO must ensure compliance with the Data Protection Act 2018 and the EU General Data Protection Regulation ("Data Protection Legislation") and the Council's own corporate retention policy.

A copy of the cancellation form should be placed on the investigation file and the original sent marked 'private and confidential' to the RIPA Co-ordinating Officer to place on the central file.

1.11 Errors in applications

An error must be reported if it is a ***relevant error*** to the Investigatory Powers Commissioner (IPC) as soon as reasonably practicable. If the error is of a serious nature then the IPC may require that the person concerned (i.e., who you intended to monitor) is informed of the error. The IPC will consider the seriousness of the error and the potential impact on the person involved, i.e., under surveillance. Legal advice should be sought as soon as possible if errors are identified. Further advice can be found in the Codes of Practice.

1.12 Magistrates Approval

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 and Criminal Procedure Rules 2012 Part 6

The Protection of Freedoms Act 2012 inserts amended sections 32A and 32B into the Regulation of Investigatory Powers Act 2000, and requires Local Authorities to have all RIPA Directed Surveillance & CHIS Applications approved by a Magistrates' Court before they can come into effect.

Once the internal authorisation has been completed, the Applicant must complete the application and draft order (*Appendix 19*) and have this reviewed by Legal Services, before submitting the application to the appropriate Magistrates' Court. Officers will need to decide whether or not to make the application in person before the Court, or whether an administrative application would be sufficient. Training and advice can be provided by Legal Services, as appropriate.

1.13 When authorisation is not required

Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance *authorisation* can be provided for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to specified grounds;
- overt use of CCTV and ANPR systems;
- certain other specific situations.

Please refer to the *Covert Surveillance and Property Interference Code of Practice* for relevant examples and guidance on the activity this covers.

CCTV and ANPR (Automatic Number Plate Recognition) Cameras

The use of overt CCTV cameras by public authorities do not normally require an authorisation under the 2000 Act. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the *Surveillance Camera Code of Practice* issued under the Protection of Freedoms Act 2012. This sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Legislation and a public authority's duty to adhere to the Human Rights Act 1998. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under the 2000 Act.

1.14 CCTV Directed Surveillance

However, if the CCTV becomes 'directed' in any way as part of a covert operation towards an individual, authorisation must be obtained. In some circumstances, police officers may ask for our cameras to be targeted at individuals or buildings, as part of their operations. In these circumstances the officer directing the CCTV should satisfy him/herself that the police have obtained proper authorisation. Surveillance carried out, as an immediate response to an event, does not require authorisation.

Surveillance activity carried out for non-criminal or disorder matters cannot be carried out under the RIPA Part II so must be authorised on the forms available in *Appendices 13-16*.

1.15 Online Covert Activity

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this Code.

Social media site investigation is a tool increasingly used by public authorities in their investigative and enforcement functions. Further guidance is contained in the Council's *Social Media Policy for Investigations*; in particular, IOs should have in mind that viewing of open source material does not require authorisation unless and until it is repeated and systematic, at which stage directed surveillance authorisation should be considered. Passing an access control so as to look at deeper into the site, for example, by making a "*friend request*" requires at least directed surveillance authorisation. If the investigation is to go further and pursue enquiries within the site, thereby established a relationship with the site host in the guise of a member of the public, this requires a CHIS authorisation. [see part 2]

Please refer to the *Covert Surveillance and Property Interference Code of Practice* for examples and guidance on relevant activity and paragraph 2.1 of this procedure below.

PART 1(a) – MONITORING AT WORK (NON-RIPA)

In general terms RIPA is not required for monitoring of staff. The relevant legislation relating to this falls under the Data Protection Legislation, Employment Practices Codes and Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018. Expectations under DPA are that much the same considerations e.g. proportionality, record of authorisation from senior officer etc. are given. Furthermore, good practice would expect clear notices to staff advising of monitoring policy, defining acceptable practices in policies e.g. IT Code of Conduct and Terms & Conditions of Employment.

Core Principles:

- It will usually be intrusive to monitor your workers.
- Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment.
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified. In any event, workers' awareness will influence their expectations.

General monitoring of staff can be defined as:

- Monitoring electronic communications – this deals with the monitoring of telephone, fax, e-mail, voice-mail, internet access and other forms of electronic communication.
- Video and audio monitoring – some (though not all) of the data protection issues that arise when carrying out video monitoring in public places will arise in the workplace. Employers carrying out video monitoring of workers will therefore find the guidance in the Information Commissioner's CCTV Code useful. Audio monitoring means the recording of face-to-face conversations, not recording telephone calls.

See **CCTV | ICO** and search for the CCTV Code of Practice.

Interceptions are authorised for:

- *monitoring or recording communications – to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training);*
- *in the interests of national security (in which case only certain specified public officials may make the interception);*
- *to prevent or detect crime;*
- *to investigate or detect unauthorised use of telecommunication systems, or*
- *to secure, or as an inherent part of, effective system operation; monitoring received communications to determine whether they are business or personal communications; monitoring communications made to anonymous telephone helplines.*

Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made.

The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: they are not prohibited by the Act.

Within the London Borough of Camden, this general monitoring is covered by:

Terms and Conditions of Employment
IT Code of Conduct
Code of Conduct
Financial Regulations

Covert Monitoring of Staff

Covert monitoring means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place. This sub-section is largely directed at covert video or audio monitoring, but will also be relevant where electronic communications are monitored when workers would not expect it.

Senior management should normally authorise any covert monitoring. They should satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection.

Any considerations must be made in line with the Investigatory Powers Act 2016 and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018.

Key points

A pre-screening Data Protection Impact Assessment (DPIA) should be performed in the first instance to set out the details of the monitoring activities. This process will assist in

identifying any privacy risks to the individual you are proposing to monitor. As a result of the pre-screening, a full DPIA may be required.

The pre-screening DPIA form can be found here.

All covert monitoring must follow the same application and authorisation procedure as defined at Part 1 – Directed Surveillance using the "General" forms shown at Appendices 10-13.

Covert monitoring should not normally be considered. It will be rare for covert monitoring of workers to be justified. It should therefore, only be used in exceptional circumstances. Ensure that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe and that the covert monitoring does not continue after the investigation is complete.

PART 2 – COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

This is a sensitive and difficult area of activity. Advice should be sought from the RIPA SRO prior to any authorisations being issued.

All IOs and AOs must refer to the Covert Human Intelligence Sources – Revised Code of Practice for examples and guidance when completing an application.

2.1 Use of a Covert Human Intelligence Source

An IO may consider it necessary to enlist the help of a third party to assist with an investigation. In such circumstances, the third party is known as a Covert Human Intelligence Source (CHIS).

Under Section 26(8) of the Act a person is a CHIS if they:

(i) Acts as an undercover officer or informant tasked with forming a relationship with a subject with the intention of obtaining personal information about them.
(ii) Establish or maintain a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
(iii) Act in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

All operations involving a CHIS must be approved, prior to a request for authorisation, in principle by the Team Leader or Investigation Manager. The purpose of this in principle approval is to ensure that officers handling and controlling the CHIS are doing so with proper authorisation and training. After initial approval, the officer requesting the CHIS must complete either a CHIS application form (*Appendix 6*) for criminal investigations or a General Purposes CHIS application form (*Appendix 14*) for civil or non-criminal employee investigations. This form must be authorised by an Authorising Officer.

As a general rule the Council will not use vulnerable individuals or persons under the age of 18 as a CHIS. There are special provisions for the use of vulnerable and juvenile sources and legal advice should be sought prior to their use.

There is no need to seek authority where the information source is a member of the public who freely provides information that has come to them during their normal activities, for example, where we ask a neighbour to keep a nuisance or harassment diary while going about their normal daily activities. However, authority must be obtained if the IO directs the CHIS activities.

If an IO considers it necessary to use a CHIS as part of an investigation, s/he must complete an Application for Authorisation of the Use or Conduct of a Covert Human Intelligence Source form, see *Appendix 6*.

2.2 Online Covert Activity

The use of the internet may be required to gather information prior to and/or during a CHIS operation, which may amount to directed surveillance. Alternatively, the CHIS may need to communicate online, for example, this may involve contacting individuals using social media websites. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an appropriately worded CHIS authorisation that includes the acquisition of this information must be sought, as set out elsewhere in the code.

Further guidance on social media can be found in the Council's *Social Media Policy for Investigations*.

2.3 Public authority responsibilities

Public authorities should ensure that arrangements are in place for the proper oversight and management of CHISs, including appointing individual officers as defined in Section 29(5)(a) and (b) of the 2000 Act for each CHIS.

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

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS, and
- monitoring the CHIS's security and welfare.

The person referred to in Section 29(5)(b) of the 2000 Act, (Controller), will be responsible for the general oversight of the use of the CHIS.

Controllers cannot be the AO, as they are separate and distinct statutory roles. Handlers will normally be at least one management tier below the Controller. This may or may not be the IO.

In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities; in either case, record keeping will be required.

2.4 Security and welfare

Any public authority deploying a CHIS should take into account of their safety and welfare when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the AO 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. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered.

The Handler is responsible for bringing to the attention of the Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS, and
- the safety and welfare of the CHIS.

Where deemed appropriate, concerns about such matters must be considered by the AO, and a decision taken on whether or not to allow the authorisation to continue.

2.5 Authorising the use of a CHIS

The decision on whether or not to authorise the CHIS rests with the AO. Full details must be included in the authorisation form of the reason for the use of CHIS and outcomes which the CHIS activity is intended to produce. Officers must give significant thought to **collateral intrusion** (i.e. those who are unconnected with the subject, who may be affected by the CHIS and what private information may be gleaned about them). The authorisation request should be accompanied by a risk assessment form detailing how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is, at all times, a person with the responsibility for maintaining a record of the use made of the source.

The use of the CHIS must be **proportionate** to the offence being committed. It should also be used only when other methods of less **intrusive** investigation have been attempted or ruled out by the potential for compromise. The application form must include details of the resources to be applied, the anticipated start date and duration of the CHIS activity, if necessary, broken down over stages. CHIS authorisation forms should include enough detail for the AO to make an assessment of **necessity** and **proportionality**. Each request should detail the nature of the source activity and the tasking which is to be given.

2.6 Magistrates Approval

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 and Criminal Procedure Rules 2012 Part 6

The Protection of Freedoms Act 2012 inserts amended sections 32A and 32B into the Regulation of Investigatory Powers Act 2000 and requires Local Authorities to have all RIPA Directed Surveillance & CHIS Applications approved by Magistrates' Court before they can come into effect.

Once the internal authorisation has been completed, the Applicant must complete the application and draft order (*Appendix 19*) and have this reviewed by Legal Services before submitting the application to the appropriate Magistrates' Court. Officers will need to decide whether to make the application in person before the Court, or whether an administrative application would be sufficient. Training and advice can be provided by Legal Services, as appropriate.

2.7 Use of a CHIS in non-criminal cases

The use of a CHIS will normally be part of an on-going criminal investigation. Even if the matter is not or has no likelihood of being a criminal investigation a General CHIS Authorisation Form must be completed, see *Appendix 16*. All of the same principles will apply when considering the use of CHIS for non-criminal matters, although authorisation is not given under RIPA Part II.

With regard to employees, the Council still has to consider an employee's right to privacy during a disciplinary investigation. Unlawful interference of the right to privacy may render the evidence obtained unusable in a criminal court. It should not affect evidence submitted to disciplinary panels. However, the process of authorisation is still needed to show that the council has not used a CHIS without proper consideration. In addition, if a CHIS is used without authorisation, the Council, and possibly individuals, may be sued for damages for a breach of human rights. Furthermore, an appeal tribunal may draw adverse inferences from such unlawful interference.

Where investigations concern only civil matters, for example, tenancy investigations where the Council intend only to recover property, the use of the CHIS may be justified for the protection of rights of others (e.g. a fraudulent tenancy or illegal sub-let is depriving others on the waiting list of a home).

2.8 Tasking a CHIS

Each CHIS will be managed through a system of tasking and review. Tasking is the assignment given to the CHIS by either the *Handler* or *Controller*. The task could be asking the CHIS to obtain information, to provide access to information or to otherwise act for the benefit of the Council. The Handler is responsible for dealing with the CHIS on a day to day basis, tasking them, recording the information provided by the CHIS and monitoring the CHIS's security and welfare. The Controller will have general oversight of these functions.

A CHIS may wear or carry a surveillance device for the purpose of recording information. The CHIS may not leave devices on the premises after they have departed, as this would constitute intrusive surveillance.

In some instances, the tasking given to a person 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. Alternatively, a trading standards officer may be involved in the test purchase of items that have been labelled misleadingly or are unfit for consumption. In such cases, it is for the IO and AO to determine where, and in what circumstances, such activity may require authorisation.

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's task. If this changes, then a new authorisation may need to be sought.

It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen actions 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 and re-authorised (for minor amendments only) or it should be cancelled and a new authorisation obtained before any further such action is carried out.

Similarly where it is intended to task a CHIS in a new way or significantly greater way than previously identified, the persons defined at as the Handler or Controller must refer the proposed tasking to the AO, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

2.9 Length of authorisation

Written CHIS authorisations last for a maximum of twelve months. They may be renewed prior to the end of the 12-month period. Activity should be cancelled as soon as it is no longer required. CHIS authorisations should not be left in place once cancellation becomes appropriate. However, if a juvenile or vulnerable CHIS is used, the duration of the authorisation is limited to four months.

In all cases, regular reviews should be carried out and normally be on a monthly basis from the date of authorisation. However, the frequency of the review should be stipulated by the AO based on the level of risk and the nature or extent of intrusion into the private lives of the subject. If a risk assessment has been conducted and if appropriate, the review period can be extended to take place every three, or even four, months from the date of authorisation.

2.10 Reviews

The AO should ensure that they review the authorisation on a regular basis in order to satisfy themselves that authority should continue. Each operation should be reviewed after

the key stages have been completed. The responsibility for the review rests with the AO. Details of the review should be recorded on an appropriate form and retained with the original authorisation held by the RIPA Co-ordinating Officer, a copy should also be held on the investigation file. Cases should be reviewed at no more than one-month intervals. Evidence of this review should be completed on the Review of the Use of a CHIS Form, see *Appendix 7*.

2.11 Renewals

There may be circumstances where the investigation requires a CHIS for a period longer than twelve months. In such cases, it will be necessary for the IO to obtain a renewal of authority from the AO and, in common with an initial authorisation, it will also need to be approved by a magistrate. A copy of the Application to Magistrate for RIPA Form, is available at *Appendix 19*.

The IO should submit a renewal form with a copy of the original Application for Authorisation of the Use or Conduct of a CHIS to the AO. A copy of the Application for Renewal of the Use or Conduct of a CHIS Form, is available at *Appendix 8*.

The AO must review both documents to ensure that there is continuing justification for surveillance. A copy of the renewal and the magistrates' approval forms should be placed on the investigation file and the original sent marked 'private and confidential' to the RIPA Co-ordinating Officer to place on the central file.

2.12 Cancellations

The use of a CHIS should be no longer than necessary to gather the required information. The AO must cancel the authorisation if satisfied that the use of the CHIS is no longer required by completing a Cancellation of the Use or Conduct of a CHIS Form, see *Appendix 9*.

A copy of the cancellation form should be placed on the investigation file and the original sent marked 'private and confidential' to the RIPA Co-ordinating Officer to place on the central file.

PART 2(a) – TEST PURCHASES

The original Code of Practice for test purchasing was published in 2002; it was an attempt to bring together the practice of the day and updated the original Home Office guidance contained in circular 17/1992.

Changes in particular to alcohol licensing legislation have prompted a significant growth in the number of test purchase operations carried out by some local authorities and have also encouraged partnership working with other organisations, most notably, the Police. Other significant changes include an increase in the availability and use of Proof of Age Cards by young people, which again has an impact upon the nature of test purchase operations. There have also been a number of decided legal cases in this area.

The RIPA policy has been updated to reflect changes in relation to test purchasing; the Home Office's RIPA Codes of Practice should also be referred to as they are regularly updated and contain helpful operational scenarios relating to test purchasing.

Officers responsible for the management of test purchasing exercises should consider – in association with the local authority's policy and the views of the Authorising Officer – the provisions of section 26(2) RIPA (in particular, whether the activity is likely to result in the obtaining of private information about any person) and section 26(8) RIPA (in particular, whether the test purchaser establishes or maintains a personal or other relationship with the seller).

Clearly, in test purchasing operations, where it is the view of the manager and Authorising Officer that it is not likely to result in the obtaining of private information and no relationship will be established then RIPA authorisation is not required.

In circumstances where the exercise is considered to fall outside the scope of RIPA, applicants should complete a "General Application for Authorisation of the Use or Conduct of a CHIS" form at *Appendix 14*.

IO's are expected to follow the CHIS Procedure as detailed in paragraphs 2.3 to 2.12 in conjunction with the specific LACORS Test Purchase Guide at *Appendix 18*.

PART 3 – COMMUNICATIONS DATA

All IOs must refer to the Communications Data – Code of Practice for examples and guidance when completing an application.

3.1 What is communications data?

The Investigatory Powers Act 2016 (IPA) regulates access to communications data.

Communications data includes the 'who', 'when', 'where', and 'how' of a communication but not the content, i.e., what was said or written. It includes the way in which, and by what method, a person or thing (i.e., computer, mobile phone, etc.) communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning.

It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

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

*NB – It **does not** include the contents of any of the communications. There is no legal means for the Council to 'intercept communications data' under the IPA.*

Local authorities are not permitted to apply for the following data:

- Internet Connection Records.
- Content of data communications, e.g., content of text messages, emails, etc.

Similar to applications for covert surveillance under RIPA, applicants must demonstrate **necessity** and **proportionality**. Applications for the acquisition of communications data should only be made where it is **necessary** for an *Applicable Crime Purpose*, as defined by Section 60(A) of the IPA and that it is **proportionate**. Consideration must also be given to any **collateral intrusion**.

This allows for applications to be made for **Entity Data**, previously referred to as subscriber data, where the purpose of obtaining the data is for the prevention and detection of crime. This definition permits the obtaining of Entity Data for 'any' crime, irrespective of seriousness.

Applications for **Events Data**, previously referred to as service or traffic data, requires a higher standard, and applications for this data should only be made were the purpose is the *prevention and detection of* ***serious crime***. Serious crime is defined in Section 86(2A) of the IPA.

Further information on Entity Data and Events Data can be found in Communications Data – Code of Practice.

3.2 Making an application

From October 2014, all applications for communications data **must** be channelled through the *National Anti-Fraud Network (NAFN)*.

If an IO considers it necessary to obtain communications data as part of an investigation, he or she must complete an application for requiring communications data to be obtained and disclosed, see 3.5 below. All requests for communication data must be made in writing.

The form must record why the IO considers this data **necessary** and **proportionate** to what is to be achieved, (and include any source material.

3.3 Role of the Approved Rank Officer (ARO)

The ARO's role is to have an awareness of the application made by the IO and convey this to the NAFN Single Point of Contact (SPoC).

Unlike the AO role with RIPA, the ARO does not authorise or approve any element of the application – only to acknowledge its existence. However, before acknowledging the application, the ARO may wish to review the **necessity** of the communications data in addition to ensuring it is **proportionate** to what it is sought to achieve.

3.4 Office for Communications Data Authorisations (OCDA)

The OCDA is the independent body responsible for the approval and assessment of all communications data applications under the IPA. They undertake the following roles:

- Independent assessment of all communications data applications;
- Approval of any appropriate applications, and
- Ensuring accountability of local authorities in the process and safeguarding standards.

3.5 National Anti-Fraud Network (NAFN)

As a result of the Data Retention and Investigatory Powers Act 2014, the Home Office revoked all accreditation that currently enables local authority staff outside of NAFN to acquire communications data. During the passage of this legislation the Government decided, in line with the recommendation from the Commissioner, to make provision to ensure that all local authorities who wish to continue to be able to access communications data only do so via NAFN's SPoC services.

The NAFN SPoC is an individual specifically trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority, the OCDA and the telecommunications and postal operators.

If not already done so, all applicants must first register with NAFN. Joining instructions are available on the RIPA intranet page.

The communications data application process is as follows:

- After logging onto the NAFN website, applicants complete the application form by first selecting the CycComms tab on the main page and then selecting "*new form*".

- Once the form is completed, the applicant submits this to NAFN. The NAFN SPoC will then review the application for legal compliance and, where necessary, provide feedback by returning it to the applicant with comments and advice for amendments. The applicant will then resubmit the form to the NAFN SPoC who will then submit for authorisation to the OCDA.

- Where rework is required, the application will be returned to the applicant, via the NAFN SPoC and the applicant will have 14 calendar days to rework the application and resubmit. **Failure to rework the application within the 14 days will result in the application being automatically rejected.**

- The OCDA will independently assess each application and will undertake one of the following actions:
    - Authorise the application;
    - Require reworking of the application, or
    - Reject the application.

Where the OCDA rejects an application, the Council has three options:

- Cease to proceed with the application;
- Re-submit the application with revised justification and/or revised course of conduct to acquire the data, or

- Re-submit the application without alteration and request a review of the decision by the OCDA.

In the case of seeking a review, or affectively appealing against the original determination, the Council has 7 calendar days to seek the review. Any appeal must be made by the RIPA SRO. The OCDA will provide guidance on this process.

A NAFN RIPA information sheet is available on the RIPA intranet page.

3.6 Notices in pursuance of an authorisation

The giving of a Notice is appropriate where a telecommunications operator or postal operator can retrieve or obtain specific data, to disclose that data, and the relevant authorisation has been granted. A Notice may require a telecommunications operator or postal operator to obtain any communications data, if that data is not already in its possession.

For local authorities, the role to issue Notices to telecommunications/postal operators sits with the NAFN SPoC and it will be their role to ensure Notices are given.

3.7 Duration of authorisations and Notices

An authorisation becomes valid on the date the authorisation is granted by the OCDA and remains valid for a maximum of one month. Any conduct authorised or Notice served should be commenced and/or served within that month.

Any Notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled.

All authorisations should relate to a specific date(s) or period(s), including start and end dates, and these should be clearly indicated in the authorisation.

Where the data to be acquired or disclosed is specified as *current*, the relevant date is the date on which the authorisation was granted. Please note that where a date or period cannot be specified other than for instance; 'the last transaction' or 'the most recent use of the service', it is still permitted to request the data for that unspecifiable period.

Where the request relates to specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date of authorisation.

3.8 Renewals and cancellations

All Notices for disclosure of communications data are subject to cancellation requirements, if the information is no longer required. However, it should be noted that all Notices have a validity of a maximum of one month.

A valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation and takes effect upon the expiry of the original authorisation. This may be appropriate where there is a continuing requirement to acquire or obtain data that may be generated in the future.

The applicant will need to consider whether the application for renewal remains **necessary** and **proportionate** and should reflect this in any renewal application made. The OCDA will need to consider this carefully in authorising any renewal.

As soon as it is no longer **necessary,** or no longer **proportionate** to what is being sought to be achieved, a cancellation of an authority must be completed. The duty to cancel rests with the NAFN SPoC.

The NAFN SPoC must ensure that the relevant postal or telecommunications operator is informed of the cancellation.

NB – Please ensure that all paperwork relating to the application is placed in the investigation file and copies be emailed to the RIPA Co-ordinating Officer to place on the central file.

3.9 Recordable and reportable errors

Where the error results in communications data being acquired or disclosed incorrectly, a report must be made to the IPC by whoever is responsible for it, i.e., ***reportable error***. For example, the telecommunications operator must report the error if it resulted from them disclosing data not requested, whereas if the error is because the public authority provided incorrect information, they must report the error. The RIPA SRO would be the appropriate person to make the report to the IPC.

Where an error has occurred before data has been acquired or disclosed incorrectly, a record will be maintained by the public authority, i.e., ***recordable error***. These records must be available for inspection by the IPC.

Further guidance and a non-exhaustive list of reportable and recordable errors can be found in the *Communications Data – Code of Practice*.

3.10 Notification of serious errors under the IPA

There may be rare occasions when communications data is wrongly acquired or disclosed and this amounts to a ***serious error***. A serious error is anything that 'caused significant prejudice or harm to the person concerned.' It is insufficient that there has been a breach of a person's human rights. In these cases, the local authority which made the error, or established that the error had been made, must report the error to the RIPA SRO and the IPC.

When an error is reported to the IPC, they may inform the affected individual subject of the data disclosure, who may make a complaint to the Investigatory Powers Tribunal (IPT). The IPC must be satisfied that the error is a) a serious error AND b) it is in the public interest for the individual concerned to be informed of the error.

Before deciding if the error is serious or not the IPC will accept submissions from the local authority regarding whether it is in the public interest to disclose. For instance, it may not be in the public interest to disclose if to do so would be prejudicial to the 'prevention and detection of crime'.

PART 4 – RECORD KEEPING & MONITORING

4.1 Record keeping

To comply with the requirements of the IPCO, Camden Council must maintain a central file containing all authorisations, reviews, renewals and cancellations.

In all instances as stated above, IOs should contact the RIPA Co-ordinating Officer to obtain a Unique Reference Number (URN) at the start of the application process. This URN must be written on the form in the box provided. IO's are responsible for ensuring that all the relevant original forms are forwarded to the RIPA Co-ordinating Officer, and for maintaining copies on the investigation file.

The RIPA Co-ordinating Officer will ensure a confidential central file is maintained as required of the IPCO. Forms relating to the authorisation for the use of a CHIS will be held on a separate file along with the risk assessment form. A central file will be maintained for the CHIS, Handlers and Controllers and this will also be held by RIPA Co-ordinating Officer. In addition, individual Control Sheets will be maintained for directed surveillance, CHIS and communications data. This sheet will include information on the authorisations, reviews, renewals and cancellations as well as indication of any **confidential information** obtained.

All applications (including those refused by an AO), authorisations, renewals and cancellations must be retained until they have been inspected by the IPCO (inspections are usually performed by IPCO every two or three years). Once the records have been inspected by IPCO, they should be disposed of by using the Council's confidential waste bins, or if the record is stored electronically, deleted from all relevant folders. Records should be disposed/deleted seven years after the investigation has closed, or after 10 years if the investigation had resulted in a successful prosecution.

Confidential information is defined as medical, religious, legally privileged material, constituent information and confidential journalistic information. If this is acquired during the course of an operation it needs to be reported to the IPCO for a higher level of authorisation.

4.2 Monitoring and quality

The RIPA Co-ordinating Officer and the RIPA SRO will review a sample of the authorisation forms on a regular basis and where necessary provide feedback/suggestions to the IOs/AOs to ensure all authorisations meet the required standard.

4.3 Identifying authorities

A sequential numbering system to simplify the central filing will be introduced to enable ease of identification. The RIPA Co-ordinating Officer will supply a unique reference number (URN) at the outset of the application for authorisation that all departments will be required to use. An authorisation will be identified in the following manner:

Directorate/Service/Investigation case no./authorisation number (see examples below)

CS/AUD/xxxxx/01
SC/TS/xxxxx/xx
SC/HIT/xxxxx/xx

NB – Additional identification numbers as highlighted below should be inserted on forms by the IO to identify the type of form. See examples below.

Reviews	**Renewals**	**Cancellations**
Insert 'RV' before the authorisation number (e.g. CS/AUT/0011/RV0225**)**	**Insert 'RN' before the authorisation number (e.g. SC/TS/xxxxx/***RN01***)**	**Insert 'C' before the authorisation number (e.g. SP/TS/xxxxx/***C07***)**

RIPA Senior Responsible Officer (SRO):
Nasreen Khan
Head of Internal Audit, Investigations and Risk Management

RIPA Co-ordinating Officer:
Kam Wong
Principal Investigator

Appendix 1 – List of Authorising Officers/Approved Rank Officers (as of April 2023)

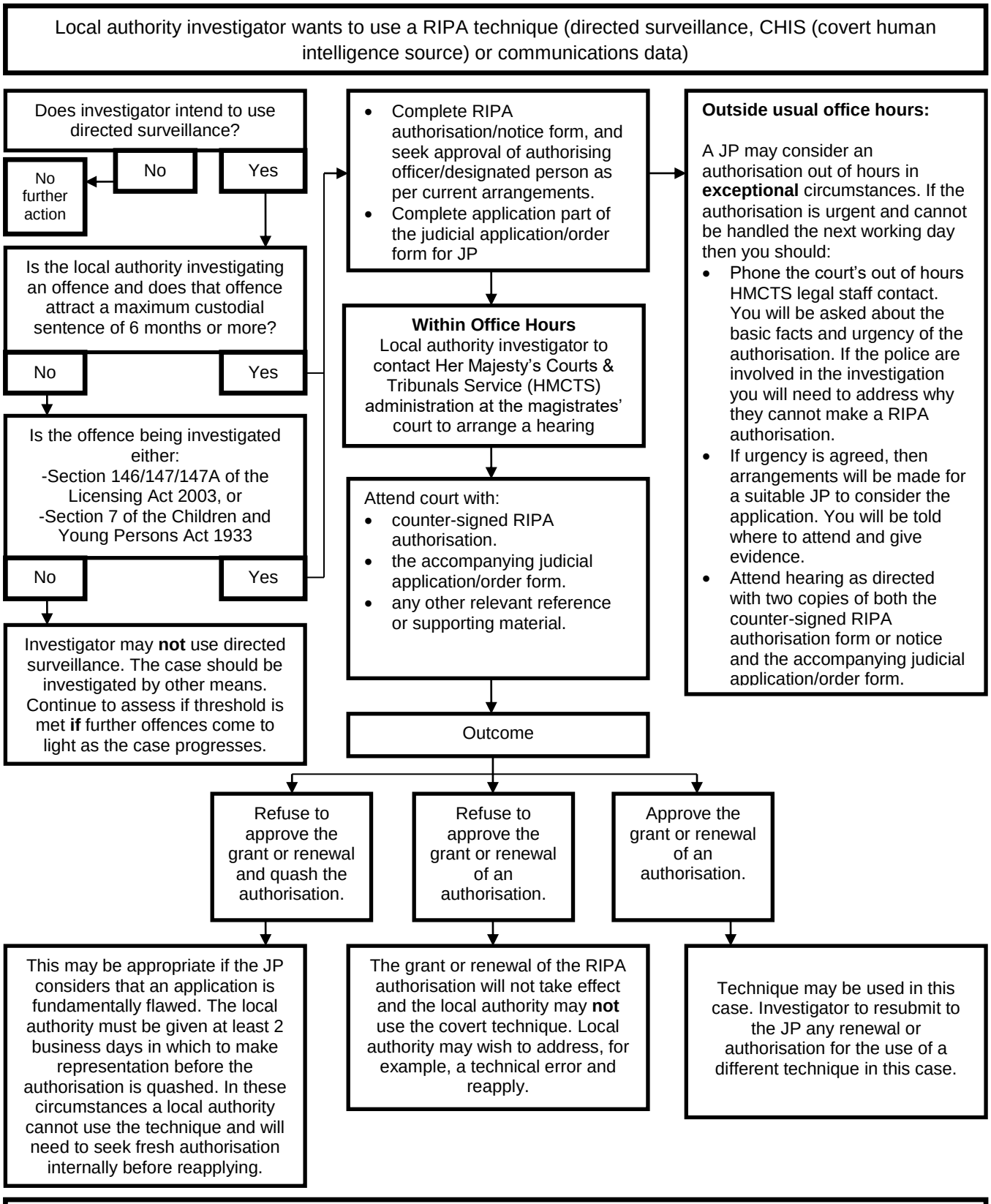
Position	Authorising Officers	Level of Authority*
Chief Executive	Jenny Rowlands	1
Director of Housing Services	Glendine Shepherd	2
Director of Public Safety	Jamie Akinola	2

***Key to Level of Authority**

1	Head of Paid Service (Chief Executive) - Children/Vulnerable Adults or where confidential information is likely to be obtained
2	Executive Directors/Directors – All other authorisations including CHIS

Appendix 20

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



Appendix 21 – Flow chart showing the RIPA authorisation procedure