

London Borough of Croydon

Corporate Policy & Procedures managing the use of Covert Surveillance Authorised under the Regulation of Investigatory Powers Act & Unregulated Activities

Index

- 1.0 Introduction**
- 2.0 Purpose of the Policy & Procedures**
- 3.0 Implementation**
- 4.0 Basic Requirements**
- 5.0 Judicial Approval**
- 6.0 Types of Surveillance**
- 7.0 Authorisation and Duration**
- 8.0 Urgent Authorisations**
- 9.0 Equipment**
- 10.0 Health & Safety**
- 11.0 Evidence**
- 12.0 - 13.0 Covert Human Intelligence Sources (CHIS)**
- 14.0 Test Purchasing**
- 15.0 Requests to undertake Covert Surveillance using the Council's CCTV**
- 16.0 Noise Nuisance Investigations**
- 17.0 Social Media**
- 18.0 Surveillance in respect of 'Non-Core' Activities or those not meeting the Criminal Threshold and Staff surveillance**
- 19.0 Access to Communications Data**
- 20.0 Requesting Authorisation to Undertake Directed Surveillance or Use of CHIS**
- 21.0 Authorising Officers**

22.0 Security of Documentation & Communications

23.0 Consequential Amendments

Annex A

1.0 Introduction

1.2 RIPA and the Human Rights Act

The Regulation of Investigatory Powers Act (RIPA) legislates for the use by local authorities of covert methods of surveillance and information gathering to assist the detection and prevention of crime in relation to an authority's core functions. **Evidence obtained by any covert surveillance or use of covert human intelligence sources could be subject to challenges under Articles 6 (right to a fair trial) and 8 (right to a private and family life) of the European Convention on Human Rights (ECHR) - the right to respect for private and family life. However, properly authorised covert surveillance under RIPA makes lawful what might otherwise be a breach of Articles 6 and 8 of the ECHR and protects the Council from any civil liability.**

1.3 Using these powers, the Council is able to:

- Acquire data relating to communications (subscriber information);
- Carry out surveillance;
- Use covert human intelligence sources (CHIS).

1.4 While some members of the community may consider RIPA to be intrusive, it is a vital tool for this Council's work to undertake a number of its core functions for example (and not exclusively) counter fraud, trading standards investigations and managing environmental issues (i.e. fly tipping). The 'core functions' were referred to by the Investigatory Powers Tribunal (*C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006*) as the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.). A public authority may only engage RIPA when in performance of its 'core functions'. For example, the disciplining of an employee is not a 'core function'.

1.5 Some of the Council's enforcement functions will require the use of covert surveillance or CHIS but the community must be confident that this is undertaken in accordance with the law is necessary, proportionate, and undertaken with the minimum of intrusion into an individual's private life.

1.6 The Council is fully committed to complying with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (as amended by the Protection of Freedoms Act 2012) (RIPA). To ensure compliance all covert directed surveillance, and use of covert human intelligence source (CHIS), falling within the scope of the Act, carried out by officers of the

Council or contractors acting on the Council's behalf, must be properly authorised by a Designated Authorising Officer.

2.0 Purpose of the Policy & Procedures

- 2.1 To comply with RIPA, it is vital that officers carrying out activities under its powers must have full regard to the codes of practice and guidance issued by the Home Office, Office of the Surveillance Commissioner and the Interception of Communications Commissioner.
- 2.2 Investigations which fall within the scope of the RIPA, but which are not correctly authorised could leave the Council open to legal challenge by individuals who consider that there has been an intrusion into their private lives or infringement of their right to a fair trial.
- 2.3 The purpose of the Council's policy and procedure on RIPA, is to reinforce the requirements of the RIPA, and relevant Codes of Practice, provide guidance to officers to minimise the risk of legal challenge to the Council and protect the rights of individuals. This policy covers those activities, which are authorised conduct under RIPA.
- 2.4 **Any failure to comply with the policy and procedures set out in this document may be considered a disciplinary offence.**

3.0 Implementation

- 3.1 This policy and procedure replaces any previous policies and procedures, and applies to all Council staff. The Council's standard contract terms and conditions require contractors to comply with all relevant policies of the Council as have been notified to it as part of the Contract. Accordingly, where any contractor may be involved in surveillance activities, this Policy and Procedure should be notified to them as part of the contracting process.

4.0 Basic Requirements

- 4.1 Under RIPA, directed covert surveillance, use of CHIS and access to communications data should only be authorised if the Designated Authorising Officer is satisfied that:
 - **SURVEILLANCE** is likely to obtain *private information*;
 - The action is **NECESSARY** for the prevention or detection of a crime (see 1.7 below); and

- Is **PROPORTIONATE** - in that it to the least extent possible the rights and freedoms (of the individual concerned and of innocent third parties), is carefully designed to meet the objectives in question and is not arbitrary, unfair or based on irrational considerations.

4.2 This requires:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime;
- Explaining how the methods adopted will cause the least possible intrusion on the subject of the surveillance and/or others;
- Considering whether the activity is appropriate use of the legislation and a reasonable way having considered all reasonable alternatives of obtaining the necessary result;
- Evidencing as far as reasonably practicable what other methods have been considered and why they were not implemented.

4.3 The proposed activity will not be proportionate if the information sought could be obtained by less intrusive means.

5.0 Judicial Approval

5.1 The Council is required to seek **Judicial Approval** before an authorisation can take effect. This is in addition to getting authorisation from one of the Council's Designated Authorising Officers. For communications, data requests the application for Judicial Approval is provided by National Anti-Fraud Network (NAFN) as part of the Single Point of Contact (SPOC) process and sent directly to the Investigating Officer. For directed surveillance and CHIS operations, the application will be prepared and submitted by the Director of Law and Monitoring Officer (Director of Law) whose representative will attend Court with the Investigating Officer when the request for Judicial Approval to proceed is sought. **See Annex A**

5.2 **Criminal Threshold** - The use of directed surveillance under RIPA is limited to the investigation of crimes, which attract a 6 month or custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco
 - See Annex A

6.0 **Types of Surveillance** (*includes monitoring, observing or listening to persons; their movements, conversations or other activities and communications*)

- 6.1 Covert Surveillance is surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.
- 6.2 Where those who are going to be targets of surveillance have been informed that surveillance will take place between a clearly specified time periods e.g. test purchases to be made for X weeks after training has been provided by the Council to retailers in respect of their responsibilities in trading in age related products. Overt use of CCTV, does not require an authorisation, and will not be considered to be covert and consequently fall outside of the RIPA regime.
- 6.3 **Local Authorities are NOT able to authorise to intrusive surveillance, or to interfere with the property of others whilst conducting directed surveillance.** Surveillance is intrusive if it 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 (visual or audio). However a surveillance device **not** on or in the premises/vehicle will only be intrusive if it consistently provides information of the same quality and detail as might be expected to be obtained for a device actually on/in the premises/vehicle.
- 6.4 For example the placing of a camera in such a manner, which provides images of the activities within residential premises, or the use of a 'tracker', attached to a private vehicle, would constitute intrusive surveillance.
- 6.5 **Directed Surveillance - is covert, but not 'intrusive'** and is undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather **private** information about them (which can include information about persons at work). Where surveillance is covert and is directed at individual(s) to obtain information about them, RIPA is likely to apply and prior authorisation must be obtained.
- 6.6 Directed surveillance must be authorised in accordance with this policy and procedure.

7.0 Authorisation and Duration

- 7.1 All requests to conduct, extend or renew a directed surveillance exercise must be made in writing on the appropriate application forms (available from the Director of Law). All requests must be submitted to a Designated Authorising Officer of the Council for their consideration and agreement before seeking a **Judicial Approval** to proceed.
- 7.2 The power to grant, extend and renew authorisations is limited to Designated Authorising officers, subject to **Judicial Approval**. Extensions should only be

granted where directed surveillance is believed by the Designated Authorising Officer to be **necessary and proportionate**. Written authorisations for directed surveillance will be valid for 3 months from the date of the authorisation or extension has been **Judicial Approved**. Designated Authorising Officers are responsible for ensuring that every authorisation is cancelled as soon as it is no longer required, with reviews as to whether, there is a continuing need for the surveillance being undertaken on a regular basis.

8.0 Urgent Authorisations

The Council has no powers to grant urgent oral authorisations to conduct surveillance.

9.0 Equipment

- 9.1 Surveillance equipment will only be installed once the necessary authorisation of the Council's Designated Authorising Officers has **Judicial Approval**. Permission to locate surveillance equipment in occupied residential premises, to undertake non-intrusive surveillance must be obtained in writing from the householder or tenant. Designated Authorising Officers shall maintain an inventory of the Council's surveillance equipment and all equipment shall be stored securely in Council premises.

10. Health & Safety

In addition to a **Judicial Approval**, a covert surveillance operation must not be commenced without detailed consideration of any insurance or health and safety applications and the necessary precautions and insurance having been put in place. Whenever practicable a site visit should always be undertaken prior to the installation of any surveillance equipment.

11. Evidence

- 11.1 During a covert surveillance operation, recorded material or information collected must be stored and transported securely. It will be reviewed regularly and access to it will be restricted to Designated Authorising Officers, the Director of Law, and the investigation officers concerned in the case.
- 11.2 The Designated Authorising Officers are responsible for deciding whether requests for access to evidence by third parties, including council officers, should be allowed and having taken legal advice where necessary. Access should generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies and/or legal

representatives (unless disclosure would prejudice any criminal enquiries or proceedings and/or an individual's right under the Data Protection Act). Designated Authorising Officers will maintain a record of all reviews of material recorded and collected covertly.

- 11.3 A register will be kept (by the senior investigating officer) of all recorded material, or information collected through the covert surveillance activities. In cases where an Interview under Caution has taken place, the material or information should be retained for at least three years from:
 - (a) The date the Investigating Officer decides that criminal proceedings are inappropriate;
 - (b) Director of Law decides the case is not suitable for prosecution;
 - (c) A court dismisses a prosecution;
 - (d) The defense or the prosecution withdraws its case;
 - (e) A court case does not proceed for any other reason.
- 11.4 Designated Authorising Officers must retain a record of the material shared with any third parties and the reasons for doing this.

12. Covert Human Intelligence Sources (CHIS)

12.1 Definition

A person is a CHIS if:

- They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything;
- if they covertly uses such a relationship to obtain information or to provide access to any information to another person; and/or
- they covertly disclose information obtained by the use of such a relationship or because of the existence of such a relationship.

12.2 A CHIS may be needed to establish or maintain a personal or other relationship for the purpose of an investigation, i.e. the person with whom the relationship is established is unaware of. A CHIS is “**tasked**” to obtain information, provide access to information or the investigation to otherwise act, incidentally, for the benefit of the relevant public authority.

12.3 Where members of the public volunteer information as part of their *normal civic duties*, e.g. an Anti-Fraud Hotline, they would not generally be regarded as a CHIS. **Similarly, a routine test purchase is unlikely to be considered a CHIS activity where the engagement of the test purchaser with those at the premises from which the test purchase is made is that of a normal transaction and does not entail establishing or maintaining a personal or other relationship.**

12.4 Consequently, the need for the use of CHIS by the Council is likely to be infrequent, however there may be **limited and exceptional circumstances** in which it is necessary to use a CHIS, and the procedures set out below must be followed if such circumstances arise.

12.5 Any designated Authorising Officer seeking guidance in CHIS related matter should contact the Director of Law.

12.6 CHIS Authorisation

12.7 As well as applying the same principles and procedures as for directed surveillance, and seeking necessary approvals there are additional considerations relating to the security, welfare and management of the source, and records relating to them which must be taken into account before the use of a CHIS can be authorised. If followed, material or information obtained from a CHIS may be used as evidence in criminal

proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.

- 12.8 Use of a CHIS may only be authorised if it is necessary for the prevention or detection of crime.
- 12.9 The Designated Authorising Officers listed in Section 20, may authorise the use of a CHIS, provided that they are satisfied that it is necessary and proportionate to do so, and that there are arrangements in place (as set out below) for managing a CHIS.
- 13.0 An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS's task. However, where it is intended to task a source in a new or significantly greater way, the handler or controller (see below) must refer the proposed tasking to the Designated Authorising Officer, who should consider whether a separate authorisation is required.
- 13.1 Applications to use, extend or discontinue the use of a CHIS must be made in writing on the appropriate authorisation forms. Written authorisations for CHIS will be valid for a maximum of 12 months from the date of authorisation or extension. As with directed surveillance, Designated Authorising Officers are responsible for ensuring that authorisation is cancelled as soon as it is no longer required, and that reviews of authorisations are carried out on at least a monthly basis.

13.2 Management of the Source

- 13.3 A Designated Authorising Officer must not seek an authorisation for the use or conduct of a CHIS unless they have appointed a person with day to day responsibility (a 'Handler') who will deal with the CHIS on behalf of the Council, direct the day to day activities of the CHIS, record the information supplied by them and monitor the security and welfare of the CHIS. A Controller with responsibility for the general oversight of them should also be appointed.
- 13.4 Meetings that take place between the Handler, Controller and/or the CHIS must be recorded, along with details of meeting between the CHIS and the subject of the investigation. Where there are unforeseen occurrences, these should be recorded as soon as practicable after the event, and the authority checked to ensure that it covers the circumstances that have arisen.

13.5 Record Keeping

- 13.6 Proper records must be kept of the authorisation and use of a CHIS, the following records must be kept when a CHIS is authorised:

- The identity of the CHIS;
- The identity, where known, used by the CHIS;
- Any relevant investigating authority other than the authority maintaining the records;
- The means by which the CHIS is referred to within each relevant investigating authority;
- Any other significant information connected with the security and welfare of the CHIS;
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a CHIS that relevant information has been considered and that any identified risks to the security and welfare of the CHIS have where appropriate been properly explained to and understood by the CHIS;
- The date when, and the circumstances in which, the CHIS was recruited;
- The identities of the persons who will act as handler, controller and person responsible for maintaining records of the use of the CHIS;
- The periods during which those persons have discharged those responsibilities;
- The tasks given to the CHIS and the demands made of them in relation to their activities as a CHIS;
- All contacts or communications between the CHIS and the Council's handler;
- The information obtained by the Council by the conduct or use of the CHIS;
- Any dissemination by that authority of information obtained in that way.

- 13.7 The Home Office Code of Practice on the use of CHIS also contains additional advice on records to be kept in relation to a CHIS. In addition to the authorisation forms, risk assessment, and the above information, a record should be kept of the circumstances in which tasks were given to the CHIS and the value of the CHIS's information in relation to the Council's investigation.
- 13.8 The records must be kept in a way that preserves the confidentiality of the CHIS and the information provided by them. The Designated Authorising Officer must not authorise the use of a CHIS until a Controller has been designated as the person with responsibility for maintaining a record of the use made of the CHIS, and arrangements are in place for ensuring that the records will be kept securely.

13.9 Safety & Security

- 13.10 Prior to authorising the use of a CHIS, the Designated Authorising Officer

shall have regard to the safety and welfare of the CHIS and shall continue to have such regard, throughout the use of the CHIS. At the outset, the safety and welfare of the CHIS after the authorisation has been cancelled or where the investigation has been closed must also be taken into account. When seeking authorisation to use a CHIS a risk assessment must be completed, to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known and provide it to the Designated Authorising Officer for consideration. This should include the nature and magnitude of any risk to the CHIS; and risks on a personal, operational and ethical basis must be considered. The risk assessment must be taken into account by the Designated Authorising Officer in deciding whether it is appropriate for authorisation to be granted for the use of the CHIS, along with the usual considerations of proportionality, necessity etc. The Designated Authorising Officer must satisfy themselves that any risks identified are justified in relation to the investigation, and that any identified risks have been properly explained and understood by the source.

- 13.11 The handler of the CHIS will be responsible for bringing any concerns about the personal circumstances of the CHIS to the attention of the controller, in so far as they may affect the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate such concerns should be brought to the attention of the Designated Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.
- 13.12 The use as a CHIS of vulnerable individuals, such as the mentally impaired, can only be authorised by the Chief Executive (or in his/her absence a Deputy Chief Executive), and **only in the most exceptional cases**. In relation to the use of juveniles as a CHIS, Designated Authorising Officers should also abide by the related Home Office Code of Practice. On no account should the use or conduct of a CHIS under 16 years of age be authorised to provide information where the relationship to which the use of the source relates is between the source and their parents (or any person who has parental responsibility) In other cases authorisation should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI2000/2793) are satisfied. These requirements relate to the presence of an appropriate adult (e.g. a parent) at meetings with the source and consideration of risk assessments. Authorisation of juvenile CHIS may only be granted by the Chief Executive (or in his/her absence a Chief Officer) and the duration of such an authorisation will be only one month, rather than twelve months.

14.0 Test Purchasing

- 14.1 This Council's need to undertake test purchasing of age restricted goods such as knives, alcohol, solvents etc, sometimes requires the use of test

purchasers who are juveniles i.e. under the age 18. Test purchasing will be conducted in accordance to the Department for Business Innovation & Skills, Better Regulation Delivery Office, and Code of Practice on Age Related Products.

- 14.2 When considering the nature of the relationship the young person, undertaking the test purchase on behalf of the Council is unlikely to be construed as a CHIS on a single transaction but this would change if the juvenile revisits the same establishment in a way that encourages familiarity. If the test purchaser wears covert recording equipment, or an adult is observing the test purchase, it will be desirable to obtain an authorisation for directed surveillance because the ECHR has construed the manner in which a business is run as private information and such an authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person. If conducting covert test purchase operations at more than one establishment, it is not necessary to create an authorisation for each premise to be visited but the intelligence must be sufficient to prevent 'fishing trips'. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises.
- 14.3 It does not follow that there must be a CHIS authorisation because designated public authorities are empowered but not obliged to authorise a CHIS. Therefore, the Designated Authorising Officer must be satisfied that they have fully considered all the relevant issues and decide whether in their opinion that a CHIS has been 'created'. If the purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.
- 14.4 Therefore, when a test purchase is considered to be necessary, it should be based on supporting intelligence that provides a weight of evidence to support it being undertaken and so that the tests of necessity, proportionality, and collateral intrusion must be carefully considered and that a demonstration that overt methods have been attempted.
- 14.5 If covert technical equipment is worn by the test purchaser, an authorisation for Directed Surveillance is required and such authorisation must identify the premises involved. If an adult is observing the test purchase and no covert technical equipment is used then the decision whether a Directed Surveillance authorisation is required will be based on a careful consideration of the circumstances of the individual case, as this is likely to be considered part of the part of the legislative functions of Council (as per the example above), as opposed to the pre-planned surveillance of a specific individuals. **Any use of** persons to undertake test purchases must be subject to risk assessment which must take account of the safety and

welfare of the test purchaser.

15.0 Requests to undertake Covert Surveillance using the Council's CCTV

- 15.1 The CCTV Control Room staff from time to time, may be requested to undertake covert surveillance on behalf of other enforcement authorities such as the Police. ALL requests must be supported by an appropriate RIPA Authorisation, from the enforcement authority and a copy of this should be provided to the CCTV Intelligence Manager before the surveillance is commenced.
- 15.2 The CCTV Intelligence Manager may refuse to provide surveillance facilities, where it is believed that information provided within the RIPA Authorisation, does not enable the requested surveillance to be conducted in accordance, with the relevant codes of practice.
- 15.3 CCTV Control Room staff will only undertake the surveillance as described within the RIPA Authorisation, and they will remain in control of the cameras and ancillary equipment at all times.
- 15.4 The CCTV Intelligence Manager shall have operational control of the surveillance being undertaken, and may choose to cease the surveillance at any time in the light of operational considerations.
- 15.6 However, surveillance request that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to obtain authorisation, which falls outside the definition of Directed Surveillance will be facilitated at the discretion of the CCTV Intelligence Manager in the light of operational considerations.

16.0 Noise Nuisance Investigations

Where covert recording of noise where the recording is decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) and/or the recording of verbal content is made at a level which does not exceed that which could be heard from the street outside or an adjoining property with the naked ear. The perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be required.

17.0 Social Media

- 17.1 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 use of social media is considered as part of an investigation, a consideration 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 investigation. Where it is considered that private information is likely to be obtained, consideration to the whether or not an authorisation is required.
- 17.2 Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.
- 17.3 If Social Media Sites are being accessed this should be done only by using a Council operated open account and generally to visit open source material only.
- 17.4 Where privacy settings are available but not applied the data may be considered open source. Even if open source sites are being reviewed, while reviewing an open source site does not require authorisation, if this is being undertaken regularly a directed surveillance authorisation may be required. Repeat viewing of open source sites may constitute directed surveillance on a case by case basis and this should be borne in mind.
- 17.5 If it becomes necessary to breach the privacy controls and become, for example "a friend" on a social media site, with the investigating officer utilising a false account concealing their identity for the purpose of gleaning intelligence, this is a covert operation intended to obtain private information and an directed surveillance authorisation should be obtained. If the investigator engages in any form of relationship with the account operator/holder then this will require a CHIS authorisation.
- 17.6 Therefore investigators when using social media to assist an investigation:
- must not 'friend' individuals on social networks, without seeking an appropriate authorisation for either Directed Surveillance, CHIS and/or both;
 - must not use their own private accounts to view the social networking accounts of other individuals;
 - investigators reviewing an individual's profile on a social networking

site should do so only once in order to obtain evidence to support or refute their investigation. Such viewing can take a backward look at the individual's profile;

- further reviewing of open profiles on social networking sites to monitor an individual's status, must only take place once an appropriate authorisation for either Directed Surveillance, CHIS and/or both has been granted;
- Investigators should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity;
- Investigators who wish to use a false identity to assist in investigation using social media can only do so once an appropriate authorisation either Directed Surveillance, CHIS and/or both has been granted;
- Investigators are forbidden from using photographs of other persons without their explicit consent to support the use of a false identity (explicit consent being an agreement in writing of how the photograph is to be used to support the investigation). Further, the safety of the person whose identity is used must be fully considered and adequate steps taken to ensure that they are not placed at risk.

18.0 Surveillance in respect of 'Non-Core' Activities or those not meeting the Criminal Threshold and Staff surveillance

- 18.1 It must be remembered that the Council is only able to seek an authorisation when using the investigation to support its 'core functions'. The 'core functions' were referred to by the Investigatory Powers Tribunal (C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006) are the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc). For example:
- A member of staff is suspected by the Council of undertaking additional employment in breach of their contract. The Council wishes to conduct covert surveillance to confirm or refute the allegation. While such activity, even if it is likely to result in the obtaining of private information, would not constitute directed surveillance for the purposes of RIPA as it does not relate to the discharge of the Council's core functions. Rather it relates instead to the carrying out of ordinary functions, such as employment,

which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and the ICO employment practices codes.

- A member of staff is claiming compensation for injuries allegedly sustained at work is suspected by the Council of fraudulently exaggerating the nature of those injuries. The Council wishes to conduct covert surveillance of the member of staff outside the work environment. Again such activity does not relate to the discharge of the Council's core functions, and therefore would not constitute directed surveillance for the purposes of RIPA as it does not relate to the discharge of the Council's core functions. Rather it relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and employment practices codes.
- A member of staff is suspected of fraudulently claiming a means tested benefit, which the Council administers. The Council wishes to conduct covert surveillance of the member of staff outside the work environment. As the administration of the means tested benefit is a core function of the Council; the proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, a directed surveillance authorisation may be appropriate.

- 18.2 Where any such surveillance is being considered, this should be dealt with in a manner similar to that of a formal authorization being sought under RIPA. A full record as to the reasoning behind the surveillance, who the surveillance was undertaken and the evidence obtained should be recorded. The Director of Law's advice must be sought prior to any such activities taking place.
Under no circumstances, whatsoever must communications data be accessed without a judicial authority, as it is only permitted to undertake directed surveillance in this manner.
- 18.3 RIPA and the Data Protection Act (DPA) (which will be replaced by the General Data Protection Regulations from May 2018) do not prevent an employer from undertaking the surveillance of their staff, but such activities must be done in a way which is consistent with the requirements of the RIPA, DPA and the General Data Protection Regulations (GDPR).
- 18.4 However, there must be a clear understanding of whether or not the use of surveillance relates to an allegation in respect of the core function of the Council or if the allegation is connected to the employment of the officer. In the former, it will generally be possible to consider an authorisation under RIPA, in the case of the latter that will not be possible.
- 18.5 Whenever, surveillance of employees is being considered advice should be

sought from the Director of Law in the first instance and the Information Commissioners Office “Employment Practices Code”, should be consulted. This Code provides useful guidance on the monitoring of staff and how this relates to their rights under DPA and GDPR.

19.0 Access to Communications Data

- 19.1 The Council has the power to gain access to communications data - that is, information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations.
- 19.2 In using such powers, officers must have full regard to the Code of Practice on Accessing Communications Data, issued by the Home Office. As with covert surveillance, access to communications data must be authorised by a designated ‘Designated Person’ and obtained via the Council’s ‘Single Point of Contact’ (SPOC) who are National Anti-Fraud Network (NAFN). Access to the NAFN website will be required for this. The Order permits access to communications data, by local authorities only where it is necessary for the prevention or detection of crime or the prevention of disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve - it should not be authorised where less intrusive means can be used to further an investigation.
- 19.3 The Council is only able to gain access to:
 - Service Data - this is information held by a telecom or postal service provider about the use made of a service by a person under investigation.
 - Subscriber Data - any other information or account details that a telecom/postal service provider holds on a person under investigation.
 - Internet Service Provider Information - Service and Subscriber Data.
- 19.4 Local Authorities are NOT authorised to obtain access to “traffic data” - information about when communications were made, who from and who to. Further, these powers do not permit access to the contents of the communication itself.
- 19.5 All requests to obtain communications data must be made using the NAFN website and will require a registered NAFN account and may only be granted

where access to communications data is to be necessary and proportionate.

19.6 Designated Persons

19.7 The posts listed in Section 20 below, detail those persons authorised by the Council to act as the Designated Person.

19.8 Single Point of Contact (SPOC) NAFN

The role of the SPOC is to:

- assess whether it is reasonably practicable to obtain the communications data requested;
- to advise applicants/Designated Authorising Officers on the types of communications data that can be obtained and associated costs;
- to check that the Form is properly completed and authorised; and
- to liaise with the service providers on obtaining the communications data requested.

19.9 NAFN manages communications data requests on behalf of the Council; with NAFN acting as the SPOC for the Council. To make a communications request applicants must first register with NAFN (www.nafn.gov.uk).

19.10 Procedure

19.11 Designated Authorising Officer will grant an Authorisation for NAFN to engage in any conduct to acquire the data. The applicant must submit the request completed on the appropriate Form to NAFN, the Council's SPOC. On receipt of the Form, the NAFN will allocate to it a unique reference number.

19.12 If NAFN is satisfied that the application has been made properly, and that the required communications data can reasonably be obtained, the application form will then be forwarded to the Council's Designated Officer for consideration. The Designated Person will then either accept or reject the request and may refuse the application (giving reasons) if they consider that the application has not been properly made.

19.13 If accepted the NAFN will fill in an Assurance of an Authorisation, this Notice must also be authorised by a Designated Officer Person before it can be served on the service provider. Once this has been done, the NAFN will serve the Notice on the Service Provider. When data is provided, the NAFN will then feed it back to the applicant or the designated person.

- 19.14 The NAFN has one month from the Authorisation being granted by the Designated Officer to request the information sought. If necessary the Authorisation can easily be renewed for a further month - it is important to note that a renewal must be granted prior to the original authorisation expiring.
- 19.15 The NAFN will record the outcome of the application on the Form and will retain as a record, the application form and notice. The NAFN will also record any cancellations of authorisations made by the Designated Person. Such records must be retained by the NAFN until such time as they have been audited by the Office of Interception Commissioners.

*****Oral applications for communications data are not permitted*****

19.16 Errors

- 19.17 The NAFN will record any errors that occur during acquisition of communications data. Such errors will be reported to the Interception of Communications Commissioner. The Director of Law is the 'Senior Responsible Officer' to oversee the reporting of errors to the Commissioner and to take steps to ensure that such errors do not reoccur.
- 19.18 There are two types of error:

- **Reportable Errors** - where an error in the application, information/communications data requested and/or information/communications supplied has resulted in the NAFN obtaining information/communications data. This error **MUST** both be recorded and reported to the Interception of Communications Commissioner; or
- **Recordable Errors** - where an error in the application or information/communications requested results in no information/communications data has been obtained by the NAFN. This error must be recorded and provided to the Interception of Communications Commissioner on request.

20.0 Requesting Authorisation to Undertake Directed Surveillance or Use of CHIS

20.1 Authorisation Procedure

- 20.2 All authorisation requests for directed surveillance or use of a CHIS, must be made by the Investigating officer using the appropriate Home Office template forms (available from the Director of Law) (including for a CHIS a

copy of the risk assessment). The Designated Authorising Officer must then consider whether the proposed surveillance is **justified, necessary and proportionate**.

- 20.3 Once the Designated Authorising Officer has completed their part of the authorisation form but before it is signed and the authorisation given:
- A hard or electronic copy of the signed authorisation form must be supplied to the Director of Law.
 - The Director of Law will review the requested authorisation and in particular advise on whether the issues of proportionality, necessity and collateral intrusion have been thoroughly considered and that the authorisation addresses the requirements of the legalisation and the Office of the Surveillance Commissioner's Code of Practice.
 - Once that advice is received, the Designated Authorising Officer must decide whether or not to grant the authorisation and seek Judicial Approval for the conduct to take place (taking into account any revisions to the authorisation as required in response to the advice from the Director of Law).
 - The Director of Law will then seek Judicial Approval – see also Annex 1.
 - If approved, the authorisation will be entered in the Central Register.

20.4 Reviews & Cancellations

- **Reviews** - Designated Authorising Officers should review on a regular basis the Directed Surveillance activity they have approved; if following a review of an active authorisation the Designated Authorising Officer believes that the Authorisation needs to be continued for a further period following the initial end date, then this will also require further Judicial Approval. A copy of the Review form as well as a Renewal Form must be supplied to the Director of Law as soon as practicable. The Director of Law will then seek Judicial Approval - see Annex 1. **This process must be completed before the expiry date of the active authorisation otherwise a new application will be required.**
- **Cancellations** - Designated Authorising Officers retain the authority to cancel an application. A copy of the cancellation form must be supplied to the Director of Law as soon as practicable.

20.5 Confidential Information

The Chief Executive (or in their absence the Director of Law) is required to authorise any activity when knowledge of confidential information (confidential personal information, legally privileged information **and** confidential journalistic material) is likely to be acquired.

20.6 Use of Contractors to Undertake Directed Surveillance on Behalf of the Council

The use of specialist contractors is permitted. When carrying out directed surveillance activities on behalf of the Council, they are only able to carry out such activities that have been authorised and use such equipment that has been stated within the authorisation. The Council's standard contract terms and conditions require contractors to comply with all relevant policies of the Council, accordingly, where any contractor may be involved in surveillance activities, this Policy and Procedure should be notified to them as part of the contracting process.

20.7 Central Record

The Director of Law will maintain a register of all requests and authorisations for covert surveillance together with reasons for any request being denied. The records in this central register will be kept for 3 years, on a rolling basis. A copy of each RIPA form is kept along with a register of the details for each authorisation (date, type of authorisation, subject of surveillance, identity of Designated Authorising Officer and dates of reviews, cancellations and renewals). The Director of Law will be responsible for monitoring authorisations and carrying out an annual review of applications, authorisations, refusals, extensions and cancellations, based on the information contained in the Central Record. RIPA forms will be checked for quality on receipt of forms for the Central Record.

20.8 Unique Reference Number Procedure

- 20.9 Each RIPA authorisation requires a Unique Reference Number (URN). The URN is used as a single reference for the life of an authorization and the Designated Authorising Officer must contact the Director of Law for a URN for each RIPA authorisation.
- 20.10 When requesting a URN the Designated Authorising Officer will be asked to provide the following information:

- Name/description of the case.

- Confirm whether it is a directed surveillance or CHIS authorisation.
 - The Designated Authorising Officer will be provided with a URN which must be used on the authorisation, review and cancellation forms relating to that authorisation.
- 20.11 The URN is not transferable i.e. if authorisation for which it has been obtained is not proceeded with then the Director of Law must be informed and the Central Register will be updated accordingly.

21.0 Authorising Officers

- 21.2 Local authority Designated Authorising Officers/designated persons are required to be, Director, Head of Service, Service Manager or equivalent levels.
- 21.3 The authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer - Head of Paid Service or, in his/her absence the acting Head of Paid Service. The Council's Designated Authorising Officers are detailed below:

Designated Authorising Officer / Designated Persons			Area of Activity
David Hogan	Head of Anti-Fraud	Resources	Directed Surveillance & the Designated Person for Acquisition of Communications Data
Simon Maddocks	Director of Governance	Resources	Directed Surveillance
Andy Opie	Director of Safety	Place	Directed Surveillance
Shayne Coulter	Head of Public Protection	Place	Designated Person for Acquisition of Communications Data

21.4 Responsibilities of Designated Authorised Officers

- Authorised Officers are personally responsible for providing copies of RIPA Authorisations to the Director of Law as soon as practicable, including 'nil returns' for the preceding month where no

authorisations have been granted.

- Where a juvenile CHIS is to be used, prior to seeking the agreement of the Chief Executive, the Director of Law must be informed to ensure that the appropriate legal advice is made available.
- 21.4 An Authorised Officer may have their authorised status rescinded at any time by the Director of Law.
- 21.5 Where an Authorised Officer becomes aware of an error in applying and/or a misuse of the application of RIPA they are required to inform the Director of Law as soon as practicable. The Director of Law will then decide upon the most appropriate course of action.

22.0 Security of Documentation & Communications

The following arrangements shall apply for the storage, retention and communication of the documents and information regarding RIPA activities.

Method of Communication / Actions	Procedure
Marking of documents	Marked OFFICIAL SENSITIVE on the top and bottom of every page.
Storage of information	Protected by one barrier, e.g. locked cabinet within a secure building, password protected file/folder on the Council network
Disposal of hard copy information	Use confidential information bins
Disposal of Removable storage devices (i.e. floppy discs, USBs, CD & DVD's.)	The disposal of these items must be carried out via the ICT Team.
Internal mail within the Council	In a sealed envelope with OFFICIAL SENSITIVE marking shown. Internal reusable envelopes must not be used
Movement of documents between externally based Council departments and/or agencies	By post or courier, in a sealed envelope. Do not show protective marking on the envelope.

Internal and public telephone networks (including the use of text messages)	May be used. Care should be taken if making calls in a public place; use guarded speech and keep conversation brief. Mobile phones may be used.
PDA's	Not to be used.
Pagers	Not to be used.
Government Secure Intranet and Email systems to be used	When available should be used.
LBC Croydon internal emails and attachments	Egress email when available should be used.
Internet emails	Not to be used
Fax	Check that recipient is on hand to receive

23.0 Consequential Amendments

The Council's Director of Law may authorise consequential amendments to this policy as a result of legislative changes or internal reorganisations within the Council.

ANNEX A

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

