LONDON BOROUGH OF MERTON

POLICY & PROCEDURE

Regulation of Investigatory Powers Act 2000 (RIPA)

London Borough of Merton
Policy date: 2010
Revised and updated: June 2020

CONTENTS

A INTRODUCTION

---

1. **OBJECTIVE: SUSTAINABLE COMMUNITIES; SAFER AND STRONGER COMMUNITIES**

Merton London Borough Council ('the Council') is committed to improving the quality of life for its residents and businesses which includes benefiting from a cleaner and more attractive physical environment. It also wishes to maintain its position as a low crime borough and a safe place to live, work and learn. Although most of the community comply with the law, it is necessary for the Council to carry out enforcement functions to take full action against those who flout the law. The Council will carry out enforcement action in a fair, practical and consistent manner to help promote a thriving local economy.

2. HUMAN RIGHTS ACT 1998 – ARTICLE 8 – RIGHT TO RESPECT FOR PRIVATE & FAMILY LIFE, HOME AND CORRESPONDENCE

The Human Rights Act 1998 brought into UK domestic law much of the European Convention on Human Rights and Fundamental Freedoms 1950. Article 8 of the European Convention requires the Council to respect the private and family life of its citizens, their homes and their correspondence. Article 8 does, however, recognise that there may be circumstances in a democratic society where it is necessary for the state to interfere with this right.

3. USE OF COVERT SURVEILLANCE TECHNIQUES AND HUMAN INTELLIGENCE SOURCES

The Council has various functions which involve observing or investigating the conduct of others, for example, investigating anti-social behaviour, fly tipping, noise nuisance control, planning (contraventions), fraud, contraventions of trading standards, licensing and food safety legislation.

In most cases, Council officers carry out these functions openly and in a way which does not interfere with a person's right to a private life. However, there are cases where it is necessary for officers to use covert surveillance techniques to undertake a specific investigation. The use of covert surveillance techniques is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), which seeks to ensure that the public interest and human rights of individuals are appropriately balanced. The Council has appointed Authorising Officers to authorise the use of two covert investigatory techniques 1) directed surveillance and 2) use of covert human intelligence source ('CHIS'). An investigating officer ('the Applicant') may **not** implement the authorisation until it has been approved by a Justice of the Peace (Magistrate). This shall require the Applicant to attend Wimbledon Magistrates' Court to make an application for an order approving the authorisation. The third investigatory technique, the acquisition of communications data, is managed by an Authorising Officer through the National Anti-Fraud Network ('NAFN').

This document sets out the Council's policy and procedures on the use of covert surveillance techniques and the conduct and use of a Covert Human

Intelligence Source. You should also refer to the two Codes of Practice published by the Government. These Codes, which were revised in August 2018, are on the Home Office website and supplement the procedures in this document.

The Codes are admissible as evidence in criminal and civil proceedings. If a provision of these Codes appear relevant to any court or tribunal, it must be taken into account.

Covert Surveillance and Property Interference Code of Practice:-
The current policy is found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf

Covert Human Intelligence Sources Code of Practice:
The current policy is found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf

4. ACQUISITION OF COMMUNICATIONS DATA

RIPA also regulates the acquisition of communications data. Communications data is data held by telecommunications companies and internet service providers. Examples of communications traffic data which may be acquired with authorisation include names, addresses, telephone numbers, internet provider addresses, geographical location of the calling or the called parties. Communications data surveillance does not monitor the content of telephone calls or emails

This document sets out the procedures for the acquisition of communications data. You should also refer to the Code of Practice which is available on the Home Office website.

Acquisition and Disclosure of Communications Data Code of Practice:
The current code of practice is found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

Overview of responsibilities

	RIPA	CHIS	Communications	Non-RIPA
Application	Applicant (service area)	Applicant (service area)	Applicant (service area)	Applicant (service area)
URN	Head of Information Governance (IG)	Head of IG	NAFN	Head of IG
Authorisation of application	Authorising Officer (AO)	AO & for identified cases (see F7 & F8) the Chief Executive	NAFN	AO
Quality assurance of application prior to court submission	SRO	SRO	N/A	N/A but seek legal advice if in doubt
Application at court	Applicant (service area)	Applicant (service area)	N/A	N/A
Review	Authorising Officer (AO)	Authorising Officer (AO)	NAFN	Applicant (service area)
Cancellation	Authorising Officer (AO)	Authorising Officer (AO)	NAFN	Applicant (service area)
Records held	Service area and central register held by Head of IG	Service area and central register held by Head of IG	NAFN	Service area and central register held by Head of IG
Register of AOs	Central register held by Head of IG	Central register held by Head of IG	N/A	Central register held by Head of IG
Details of training records	Service area and central register held by Head of IG	Service area and central register held by Head of IG	N/A	Service area and central register held by Head of IG
Retention	Central register and applications – 3 years	Central register and applications – 3 years	NAFN	Central register and applications – 3 years

	Material gathered during the surveillance operation shall be retained in accordance with section N1 and N8 sentence if longer	Material gathered during the surveillance operation shall be retained in accordance with section N1 and N8 sentence if longer		Material gathered during the surveillance operation shall be retained in accordance with section N1 and N8 sentence if longer

B AUTHORISING OFFICER RESPONSIBILITIES

1. The Council may only conduct directed surveillance under RIPA where the 'crime threshold' is satisfied and judicial approval has been granted for the operation.

2. The Council's Monitoring Officer (the Managing Director of the South London Legal Partnership) is the Senior Responsible Officer for the purposes of this policy. The Monitoring Officer has delegated powers to appoint Authorising Officers. Authorising Officers will only be appointed if the Monitoring Officer is satisfied that they have received suitable training on RIPA. The Chief Executive means the Head of Paid Services as defined within section 4, Local Government and Housing Act 1989.

3. Chief Officers of the Council and Authorising Officers in their Departments take personal responsibility for the effective and efficient observance of this document.

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

5. Authorising Officers must also pay particular attention to health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer authorise any surveillance unless, and until satisfied that

    - the health and safety of Council employees/agents are suitably addressed
    - risks minimised so far as is possible, and
    - risks are proportionate to the surveillance being proposed.

6. If an Authorising Officer is in any doubt guidance should be sought from the Chief Officer, the Council's Health & Safety Officer or Head of Law (Communities and Environment).

7. Authorising Officers should wherever practicable send an application to the Monitoring Officer for quality assurance purposes before it is submitted to court. The Authorising officer must also ensure that, when sending copies of Forms to the Monitoring Officer (or any other relevant authority), the forms are sent via email marked OFFICIAL-SENSITIVE [LEGAL].

8. Reports on the use of RIPA will be submitted quarterly to be considered by the Standards and General Purposes Committee.

C GENERAL INFORMATION ON RIPA

1. The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their homes and their correspondence.

2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-

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

3. The Regulation of Investigatory Powers Act 2000 provides the statutory mechanism for authorising covert surveillance and the use of a CHIS– e.g. undercover agents. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA and this Policy and Procedure document seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

4. Directly employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. Please refer to Section G on Authorising Officers.

5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint may be made to the Investigatory Powers Tribunal, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation.

6. A flowchart of the procedures to be followed appears at **Appendix 1**.

D WHAT RIPA DOES AND DOES NOT DO

---

1. RIPA does:

- require prior authorisation of directed surveillance.
- **prohibit the Council from carrying out intrusive surveillance**.
- require authorisation of the conduct and use of a CHIS.
- require safeguards for the conduct and use of a CHIS.
- permit the council to obtain communications data from Communications service providers

2. RIPA does not:

- make lawful conduct which is otherwise unlawful.
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information from the DVLA or from the Land Registry as to the ownership of a property.

3. If the Authorising Officer or any Applicant is in any doubt, advice should be obtained from the Monitoring Officer or Head of Law (Communities and Environment) before any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

E TYPES OF SURVEILLANCE

1. **Surveillance** includes:

- monitoring, observing and listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It may be conducted with or without the assistance of a surveillance device.

- recording anything mentioned above in the course of authorised surveillance.

- surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

2. **Overt Surveillance**

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (eg. in the case of most test purchases), and/or will be going about Council business openly.

3. Similarly, surveillance will be overt if the subject has been told it will happen for example, where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues.

4. **Covert Surveillance**

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place (section 26(9)(a) of RIPA). It cannot however be necessary if there is reasonably available an overt means of finding out the information desired.

5. RIPA regulates two types of covert surveillance, directed surveillance and intrusive surveillance and the use of Covert Human Intelligence Sources (CHIS).

6. **Directed Surveillance**

Directed surveillance is surveillance which:-

- is covert surveillance that is not intrusive;
- is carried out in relation to a specific investigation or operation in a manner likely to obtain private information about any person (whether

or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) RIPA); and*

- Other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under RIPA.

A planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about them, or any other person.

7. Private Information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationships with others, such as family and professional or business relationships. Family should be treated as extending beyond formal relationships created by marriage or civil partnerships.

8. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.

.

Example: *Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.*

9. Private information may include personal data such as names, addresses or telephone numbers. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Example: *A trading standards officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.*

10. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required.

The way a person runs their business may also reveal information about their private life and the private lives of others.

11. Privacy considerations are likely to arise if several records are examined together to establish a pattern of behaviour.

> ***Example:*** *An Environment Health Officer wishes to drive past a public house or café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation should be considered.*

12. Only officers authorised by the Monitoring Officer as Authorising Officers for the purpose of RIPA may authorise directed surveillance'

13. <u>Intrusive Surveillance</u>

Intrusive surveillance is covert surveillance that is:

- carried out in relation to anything taking place on residential premises, or
- in a private vehicle, and
- involves the presence of an individual on the premises or in the vehicle, or
- or is carried out by a surveillance device in the premises/vehicle.

Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

> ***Example:*** *An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance*

> ***Example:*** *A communal stairway in a block of flats would not be regarded as residential premises unless used as a temporary place of abode by a homeless person.*

***Example**: A front garden or driveway of premises readily visible to the public are not regarded as residential premises.*

***Example**: residential premises occupied by the Council for non-residential purposes – for an undercover operation to catch rogue traders who provide bogus services (for example, replacing a electrical consumer unit when all that is required is the replacement of a blown fuse).*

14. **Council officers and its agents may not carry out intrusive surveillance.**

15. **Intrusive surveillance may only be carried out only by police and other law enforcement agencies. Intrusive surveillance relates to the location of the surveillance, and not any consideration of the information that is likely to be obtained.**

16. "**Necessity**" – Applies in All Cases

RIPA requires that the person authorising surveillance to consider it to be necessary in the circumstances of the particular case. Therefore, Applicants and Authorising Officers must consider why directed surveillance is necessary. In addressing the issues of necessity, information should include:

- Why directed surveillance is needed to obtain information that is sought from the operation?
- Why is it necessary to interfere with an individuals' privacy using covert surveillance
- Why covert surveillance is the best option to obtain the information having considered other alternatives?
- What other methods of obtaining the information has been considered and why they have been discounted?

17. Authorising Officers may not authorise directed surveillance unless:

It is for the purpose of preventing or detecting a criminal offence AND meets the 'crime threshold'.

The 'crime threshold' is met if the purpose of the directed surveillance is:

a) to detect or prevent criminal offences for which the punishment on conviction is a term of imprisonment of not less than 6 months; or

b) the offence or the activity subject to directed surveillance constitute an offence under sections 146, 147, or 147A of the Licencing Act 2003 or section 7 of the Children and Young Persons Act 1933 (offences involving sale of alcohol and tobacco to underage children).

The crime threshold applies to directed surveillance, not to CHIS or

Communications Data authorisations.

Applications for directed surveillance should identify the offence(s) by reference to the statutory provision and penalty on conviction.

18. Proportionality

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

19. The activity will not be proportionate if it is excessive in the circumstances or if the information which is sought could reasonably be obtained by less intrusive means. All such activity must be carefully managed to meet the objective and must not be arbitrary or unfair. All those involved in undertaking directed surveillance must be fully aware of the extent and limits of the authorisation.

20. Collateral Intrusion

Before authorising directed surveillance the Authorising Officer should also take into account the risk of obtaining private information about persons who are not the subjects of the surveillance (collateral intrusion). Particular consideration should be given in cases where religious, medical, journalistic or legal privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved.

21. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to the intrusion of the privacy of the intended subject of the surveillance. All applications should include an assessment of the risk of collateral intrusion and details of any measures

taken to limit this, to enable the authorising officer to fully consider the proportionality of the proposed actions.

22. Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

23. A directed surveillance authorisation may be required to view or monitor a social media or other online account despite access being given with the consent of the owner. There will be a need to consider whether the account(s) contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered.

Activity not falling within the definition of covert surveillance

24. Some surveillance activity does not constitute directed surveillance and no directed surveillance authorisation can be obtained 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 the detection and prevention of crime (for offences satisfying the crime threshold)
- overt use of CCTV and ANPR systems;
- certain other specific situations (see paragraph F6 and G) or the covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (music, machinery or an alarm).

Immediate response

25. Covert surveillance that is likely to reveal private information about a person, but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation would not require a directed surveillance authorisation. RIPA is not intended to prevent law enforcement officers fulfilling their legislative functions. To this end, section 26(2)(c) of the RIPA provides that surveillance is not directed surveillance when it is carried out by way of an immediate response to events or circumstances, the nature of which is such that it is not reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

Example: *An authorisation under RIPA would not be appropriate where a waste enforcement in course of a routine patrol recognises suspicious activity, for example, a flatbed lorry fully laden with waste driving into the secluded part of a housing estate after 4pm on a winter's afternoon.*

General observation activities

26. The general observation duties of many enforcement officers do not require authorisation under RIPA, whether covert or overt. Such general observation duties frequently form part of the legislative functions of the Council, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

    Example: *Trading standards officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of the Council and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.*

    Example: *Intelligence gathered by the Council suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. The Trading Standards Team deploys a juvenile to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of RIPA, such that officers are likely to conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation. Different considerations may apply to a 'test purchase' carried out in a supermarket as opposed to a corner shop.*

Surveillance not relating to public functions

27. RIPA does not grant powers to carry out surveillance. It simply provides a framework that allows the Council to authorise and supervise a defined category of surveillance in a manner that ensures compliance with the Human Rights Act 1998. Equally RIPA does not prevent surveillance from being carried out in other circumstances that fall outside the RIPA framework. Further guidance is provided at section **K Non RIPA Authorisation**.

Overt surveillance cameras - CCTV and ANPR (Automatic Number Plate Recognition)

28. The use of overt CCTV cameras by the Council does not normally require an authorisation under RIPA. Members of the public are made aware that such

systems are in use 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 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner. The Council is aware of the Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information").

29. The Council has regard to the provisions of the Surveillance Camera code, where surveillance is conducted overtly by means of a surveillance camera system in a public place in England and Wales.

30. The Surveillance Camera code sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 2018 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 RIPA.

> ***Example:*** *A town centre CCTV systems is used to gather information as part of a reactive operation (for example, a flatbed lorry fully laden with waste is captured tipping its contents within a Council operated car park – the CCTV system is used to track the vehicle to observe it pass an ANPR camera so that it may be identified as being used in the commission of the offence). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.*

31. However, where overt CCTV or other overt surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or other overt surveillance cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

F CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

It is unlikely that the Council would need to use a CHIS. If it appears that use of a CHIS may be required Authorising Officers must seek legal advice from the Monitoring Officer.

Who is a CHIS?

1. 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 falling within the following:
   a) they covertly use such a relationship to obtain information or to provide access to any information to another person; or
   b) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

2. A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

3. A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question

4. RIPA generally does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information. This will depend on how the member of the public has obtained the information. If it is obtained in the course of a personal or other relationship or as a consequence of that relationship even if the relationship was not established or maintained for the purpose of obtaining the information then the informant is likely to be a CHIS. The Applicant should seek legal advice before acting on the information received from such an informant.

5. However, by virtue of section 26(8) (c) of RIPA, there may be instances where an individual covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. In such circumstances, where a member of the public, though not tasked to do so, gives information (or repeated information) about a suspect, then serious consideration should be given to designating the individual as a CHIS, particularly if the Council intends to act upon the information received. **Legal advice must be is sought in any such circumstances.**

What must be authorised?

4. The conduct or use of a CHIS requires prior authorisation.

    - **Conduct** of a CHIS means establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.

    - **Use** of a CHIS means taking action to induce, ask or assist a person to act as a CHIS and the decision to use a CHIS in the first place.

5. The Council may use CHIS's if, and only if, the RIPA procedures detailed in this document, are followed. Authorisation for CHIS's may only be granted if it is for the purposes of preventing or detecting crime or of preventing disorder.

6. The use of a recording device by a covert human intelligence source in respect of whom an appropriate use or conduct authorisation has been granted permitting him or her to record any information obtained in their presence is neither directed nor intrusive surveillance [s48(3), RIPA].

Juvenile Sources

7. Special safeguards apply to the use or conduct of juvenile sources (i.e. those under the age of 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person with parental responsibility for him or her. Only the Chief Executive, or in their absence, a Chief Officer can authorise the use of a juvenile as a source.

Vulnerable Individuals

8. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

9. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive, or in their absence, a Chief Officer can authorise the use of a vulnerable individual as a source.

Test Purchases

9. Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

10 By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally

imported products) shall require authorisation as a CHIS. Similarly, using hidden body video cameras to record what is going on in the shop may require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

11. Authorising Officers should consider the likelihood that the test purchase will lead to a relationship being formed with a person in the shop. If the particular circumstances of a particular test purchase are likely to involve the development of a relationship Authorising Officers must seek legal advice from the Monitoring Officer.

Anti-Social Behaviour Activities (eg. Noise andViolence etc)

12. Persons who complain about anti-social behaviour, and are asked to keep a diary will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be available. It such circumstances the Non-RIPA authorisation process should be followed as set out in section K Non-RIPA Activity.

13. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record without RIPA authorisation if the noisemaker is warned that this will occur if the level of noise continues. Placing a covert stationary or mobile camera outside a building to record anti-social behaviour on residential estates will require prior authorisation pursuant to the council's separate policy on camera surveillance. It will also be important to engage with the Safer Merton Team.

G Voluntary Interviews with members of the public

The recording, whether overt or covert, of an interview with a member of the public does not constitute directed nor intrusive surveillance where it is made clear that the interview is entirely voluntary and that the interviewer is a Council officer. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a member of the Council and that information gleaned through the interview will pass into the possession of the Council.

H AUTHORISATION PROCEDURES

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation as approved by the Justice of the Peace (Magistrate).

   Appendix 1 provides a flow chart of the process from application consideration to recording of information.

Authorising Officers

2. Forms can only be signed by Authorising Officers appointed by the Monitoring Officer. Officers can only be Authorising Officers if they are the Chief Executive, Chief Officers, Heads of Service, or other Unit Managers who are considered to be suitable by the Monitoring Officer. Appointments of these officers are subject to the training requirements set out in paragraph 4 below.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **Although authorisations cease effect wih time they must be formally cancelled.**

Training Records

4. The Monitoring Officer will only appoint Authorising Officers if satisfied that they have undertaken suitable training on RIPA. The Monitoring Officer shall require evidence of suitable training to be supplied usually in the form of a certificate from the relevant party to the effect that the Authorising Officer has completed a suitable course of instruction.

5. The Head of Information Governance shall maintain a Register of Authorising Officers and details of training undertaken by them.

6. If the Monitoring Officer is of the view that an Authorising Officer has not complied fully with the requirements of this document, or the training provided to him or her, the Monitoring Officer is duly authorised to withdraw that Officer's authorisation until they have undertaken further approved training or have attended a one-to-one meeting with the Monitoring Officer.

Application Forms

7. Only the approved RIPA forms may be used which are retained on the Home Office website. The forms can be found using the hypertext links in Appendices 2 and 3. With each application the relevant form should be downloaded from the Home Office website.

8. ‘A Forms’ (Directed Surveillance) – See Appendix 2

Form A 1 **Application** for Authority for Directed Surveillance
Form A 2 **Renewal** of Directed Surveillance Authority
Form A3 **Review** of Directed Surveillance Authority
Form A4 **Cancellation** of Directed Surveillance

9. ‘B’ Forms (CHIS) – See Appendix 3

Form B 1 **Application** for Authority for Conduct and Use of a CHIS
Form B 2 **Renewal** of Conduct and Use of a CHIS
Form B 3 **Review** of Conduct and Use of a CHIS
Form B 4 **Cancellation** of Conduct and Use of a CHIS

Grounds for Authorisation

10. Directed Surveillance (**A Forms**) or the Conduct and Use of the CHIS (**B Forms**) can be authorised by the Council only on the grounds of preventing or detecting crime or preventing disorder. No other grounds are available to local authorities.

Assessing the Application Form

11. The following information should be included on the application form:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in s 28(3)b of RIPA;
- the nature of the surveillance and the precise location it is to take place;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve and detail of less intrusive options that have been considered.

12. Before an Authorising Officer signs a Form, they must:-

(a) Comply with this Policy & Procedures document and the training they have undertaken

(b) Satisfy themselves that the RIPA authorisation is:-

(i) in accordance with the law**;**

(ii) (in respect of directed surveillance) that the offence being investigated satisfies the crime threshold;
(iii) necessary in the circumstances of the particular case on the ground mentioned in paragraph 10 above; and
(iv) proportionate to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information. The least intrusive method will be considered proportionate by the courts.

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion. This matter may be an aspect of determining proportionality;

(e) Make a note on the Form that the Applicant was informed of the requirement to return to have the authorisation cancelled should it be apparent (to the Applicant) the directed surveillance no longer meets the criteria upon which it was authorised. Further, a date shall be set for the review of the authorisation;

(f) Obtain a Unique Reference Number (URN) for the application from the Head of Information Governance by emailing data.protection@merton.gov.uk;

(g) Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded via email to the Monitoring Officer (or any other relevant authority), marked OFFICIAL-SENSITIVE [LEGAL], within 5 days of the relevant authorisation, review, renewal, cancellation or rejection**.**

13. For Communications and CHIS applications, the Authorising Officer should:

(a) Set a date for review of the authorisation and review on that date using the relevant form;

(b) Obtain a Unique Reference Number (URN) for the application from the Head of Information Governance by emailing data.protection@merton.gov.uk

(c) Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded via email to the Monitoring Officer (or any other relevant authority), marked OFFICIAL-SENSITIVE [LEGAL] within 5 days of any, renewal, cancellation or rejection;

(d) In the case of notices relating to communications data, these will be kept by a 'Designated Person' selected by the Monitoring Officer. The Monitoring Officer shall have access to such forms as and when required;

(e) If unsure on any matter, authorising officers should obtain advice from the Monitoring Officer, before signing any forms.

Additional Safeguards when Authorising a CHIS

14. When authorising the conduct or use of a CHIS, the Authorising Officer must also**:-**

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved.

(b) Be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

(c) Consider the likely degree of intrusion of all those potentially affected;

(d) Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(e) Ensure records contain particulars and are not available except on a need to know basis.

(f) Ensure that if the CHIS is under the age of 18 or is a vulnerable adult the Authorising Officer has to be the Chief Executive or in their absence, a Chief Officer.

The Authorising Officer must attend to the requirement of section 29(5) RIPA and of the Regulation of Investigatory Powers (Source Records) Regulations 2000. Legal advice must be obtained in relation to the authorisation of a CHIS.

15. Approval by a Justice of the Peace (JP)
Judicial approval is required before acting on the authorisation to carry out directed surveillance and conduct or use of a CHIS. Arrangement should be made to attend an Applications Court at Wimbledon Magistrates' Court. It may be appropriate to instruct the South London Legal Partnership to attend court on the Council's behalf, depending on the nature of the application and the experience of the Authorising Officer.

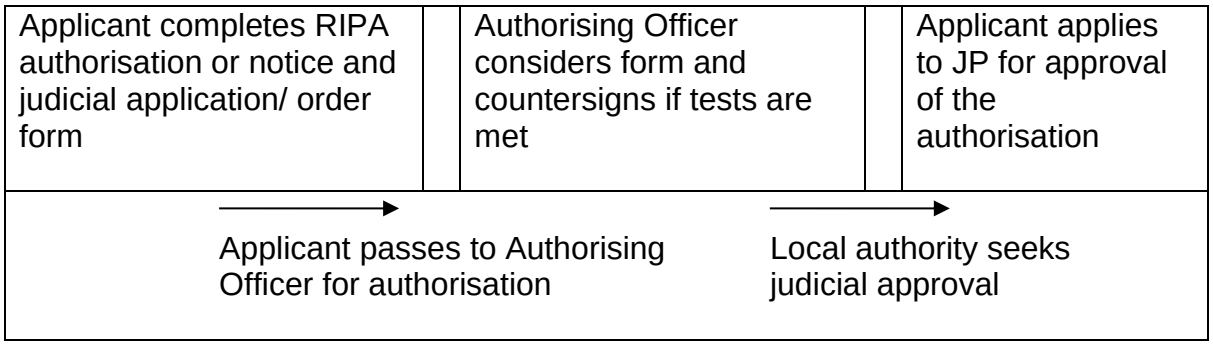
16. Judicial approval is also required on the renewal of an authorisation.

17. The JP must decide whether the grant or renewal of an authorisation should be approved and it will not come into effect unless and until it is approved by a JP (sometimes referred to as a Magistrate). Although it is possible to request judicial approval for the use of more than one technique (i.e. directed surveillance and CHIS data) at the same time, in practice, it is better to separate the applications for approval as different considerations apply to

these different techniques, this may prove to be difficult to perform with the degree of clarity required. It is recommended that separate authorisations or notices to use different RIPA techniques should be submitted.

18. Please note that the application and any renewal of the application require judicial approval. Reviews and cancellations of authorisations do not require judicial approval and remain an internal process. The process is outlined below:

Directed Surveillance / CHIS (Covert Human Intelligence Source)



The Role of the JP

19. The role of the JP is set out in section 32A RIPA (for directed surveillance and CHIS).

20. The Act provides that the authorisation shall not take effect until the JP has made an order approving such an authorisation. The matters on which the Magistrate needs to be satisfied before giving judicial approval are:

- there were reasonable grounds for the local authority to believe that the authorisation was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter;

- in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter;

- in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 20003 were satisfied and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter;

- the local authority application has been authorised by a designated person;

- the grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of section 25(3) RIPA

Duration

21. The Form must be reviewed in the time stated and cancelled once it is no longer needed. The authorisation to carry out/conduct the surveillance lasts for 3 months (from authorisation) for directed surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the authorisation is spent. In other words, the forms do not expire. The forms have to be reviewed, renewed and/or cancelled (once they are no longer required).

22. Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

23. All authorisations should be reviewed based on the level of collateral intrusion or the amount of confidential information obtained. Authorising Officers should set review dates based on the likelihood of this information being captured.

I WORKING WITH / THROUGH OTHER AGENCIES

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used by the Authorising Officer and the agency advised or kept informed, as necessary, of the various requirements. The agency must be made aware explicitly what they are authorised to do.

2. When another agency (e.g. Police, HMRC etc.):-

   (a) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Monitoring Officer for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

   (b) wishes to use the Council's premises for their own RIPA action, the Chief Officer or Head of Service should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should <u>not</u> be used as the Council is only assisting not being involved in the RIPA activity of the external agency.

3. In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other Agency <u>before</u> any Council resources are made available for the proposed use.

4. Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. It is therefore recommended that where an authorising officer considers that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation is to take place.

5. **If in doubt, please consult with the Monitoring Officer at the earliest opportunity.**

J DIRECTED SURVEILLANCE - SOCIAL MEDIA POLICY

1. The growth of the internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public it serves. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation shall not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

2. The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be sought.

3. Where an officer (or person acting on behalf of the Council) intends to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed

4. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

5. Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

6. Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by the council of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide

audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

7. Whether the Council interferes with a person's private life requires a consideration of the nature of the activity in relation to that information. Simple reconnaissance of social media and online sites (which would take the form of a preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where an officer (or third party acting on the behalf of the Council) is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

> ***Example:*** *A trading standards officer undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*
>
> ***Example:*** *A Fraud Investigator undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*
>
> ***Example:*** *A Fraud Investigator officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit.*

8. In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

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

- Whether it is likely to result in obtaining private information about a person or group of people

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

- Whether the information obtained will be recorded and retained;

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

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

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

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

9. Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

> ***Example:*** *A trading standards officer using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by the Council either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

10. Officers should be aware of the importance to verify the accuracy of information on social networking sites if such information is to be used as evidence. An individual may post information that inflates, exaggerates or embellishes the truth.

K NON-RIPA ACTIVITY

1. There may be occasions when during the course of an investigation it may become necessary to conduct surveillance of individuals in respect of matters that do not satisfy the crime threshold. For example, in relation to an investigation into an allegation that a contractor is not carrying out their work as contracted, a serious disciplinary offence by a member of staff is alleged e.g. gross misconduct, or children are at risk where Court Orders are not being respected, then a RIPA authorisation is not usually available because criminal proceedings are not normally contemplated.

2. Similarly, there may be serious cases of neighbour nuisance or involving anti-social activity which involve potential criminal offences for which the penalty is below the thresholds which would enable use of a RIPA authorisation. Nonetheless in such cases there may be strong grounds for carrying out directed surveillance or use of a CHIS. Indeed there may be circumstances in which directed surveillance or use of CHIS is the only effective means of efficiently obtaining significant information to take an investigation forward.

3. A person may make a claim or a complaint to the Investigatory Powers Tribunal should they consider the use of directed surveillance or use of a CHIS infringed their Article 8 rights. It would be then for the Council to satisfy the IPT that such infringement was justified, necessary and proportionate in pursuit of a legitimate aim. Completing the Non-RIPA application forms provides a written record of those matters taken into account at that time regarding justification, necessity and proportionality.

4. In these circumstances, the investigating officer is required to go through the RIPA authorisation process in terms of considering:

    a) Why there is no other alternative to undertaking the directed surveillance;
    b) Why the surveillance is necessary; and,
    c) How it is proportionate in the circumstances.

5. The investigating officer is required to complete a ‘non-RIPA’ authorisation form (in the same terms of a RIPA form but clearly marked ‘NON-RIPA’). The application must be submitted to an Authorising Officer for approval.

6. Where it is deemed that the above-mentioned criteria have been satisfied, the non RIPA surveillance should be monitored and reviewed in accordance with the existing Council policy. The same arrangements for RIPA authorisations are followed for Non-RIPA authorisations, that is, a Non-RIPA URN is required; the operation is subject to review and cancellation; and records are retained in the same way and are to be made available to an IPCO, if requested. In the event of a claim or complaint made to the IPT it shall be essential to have such records to demonstrate the activity was justified, necessary and proportionate.

Test purchase exercises

7. If no application for directed surveillance is made in relation to a test purchase exercise involving juveniles the ‘Non RIPA Activity’ procedure shall be followed. On completion of the test purchase exercise a written record shall be made of the review of the exercise, including an assessment of the risks of private information being obtain and the risk of collateral intrusion. Regard shall be had to the reviews before embarking on successive test purchase exercises.

L RECORDS MANAGEMENT

---

1. The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Monitoring Officer.

Records Maintained in the Department

2. The following documents must be retained by the Department authorising the surveillance:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).

Central Register maintained by the Monitoring Officer

3. Authorising Officers must forward a copy of the form to the Monitoring Officer for the Central Register, within 5 days of the authorisation, review, renewal, cancellation or rejection. The Monitoring Officer will monitor the same and give appropriate guidance to Authorising Officers from time to time, or amend this document in the light of changes of legislation or developments through case law.

4. The Council shall retain records for a period of at least three years from the ending of the authorisation for applications and for surveillance material acquired during an operation only for so long as shall be compliant with sections N1 and N8.

5. The Investigatory Powers Commissioner's Office (IPCO) can audit/review the Council's policies and procedures, and individual authorisations.

6. The Investigatory Powers Commissioner's Office will also write to the Council from time to time, requesting information as to the numbers of authorisations made in a specific period. It will be the responsibility of the Monitoring Officer to respond to such communications as well as to submit the annual return.

M Reporting Errors

1. An error must be reported to the Monitoring Officer if it is a “relevant error”. The error should be reported in the first instance to Authorising Officer who must immediately report the error to the Monitoring Officer. The Monitoring Officer shall agree with the Authorising Officer the scope and purpose of a written report to be completed within 5 days.

2. Under section 231(9) of the Investigatory Powers Act 2016, a relevant error is any error by the Council in complying with any requirements imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA. Examples of relevant errors occurring would include circumstances where:

   - surveillance activity has taken place without lawful authorisation; or

   - There has been a failure to safeguard private information, confidential or privileged information gathered or obtained pursuant to an authorisation.

3. The Monitoring Officer shall notify the Investigatory Powers Commissioner when a relevant error has occurred. The Council is required to notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

4. From the point at which the Council identifies that a relevant error may have occurred, it must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the Council must also inform the Commissioner of when it was initially identified that an error may have taken place.

5. The Monitoring Officer shall submit a full report to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report shall include information on the cause of the error; the amount of surveillance and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

6. The Investigatory Powers Commissioner may issue guidance as necessary, including guidance on the format of error reports.

N Managing information

1. Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this policy and procedure, something is necessary for the authorised purposes if the material:

   - is, or is likely to become, necessary for any of the statutory purposes set out RIPA in relation to covert surveillance;
   - is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
   - is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
   - is necessary for the purposes of legal proceedings; or
   - is necessary for the performance of the functions of any person by or under any enactment.

2. There is nothing in RIPA which prevents material obtained under directed or surveillance from being used to further other investigations where it becomes relevant and in accordance with the safeguards regarding the dissemination of material.

3. Material acquired through covert surveillance may be disseminated both within the Council and shared with other Councils, the Police or HMRC, where necessary in order for action to be taken on it. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the lawful purposes. This obligation applies equally to disclosure to additional persons within a public authority and to disclosure outside the authority. In the same way, only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

4. The obligations apply not just to the original public authority acquiring the information under an authorisation, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain the original authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients.

5. Where material obtained under an authorisation is to be disclosed to the authorities of a country or territory outside the UK, the Council must ensure

that the material is only handed over to the authorities if it appears to them that any requirements relating to minimising the extent to which material is disclosed, copied, distributed and retained will be observed to the extent that the authorising officer considers appropriate.

Storage

6. Material obtained through directed surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material. Any physical evidence - hardcopies of photographs; written records (notes and prints of digital records); hard drives; USB sticks; smart phones (until digital records are transferred) shall be retained within a secure storage with restricted access. Property records shall be maintained which include the details of when the secure storage was entered and for what purpose.

7. All such material in digital form shall be retained on a secure network with access limited to those staff that have the relevant permissions. There should be a full audit trail of any viewing, download or transfer of the information.

Destruction

8. Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purposes set out in paragraph 1 above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

9. All applicants and Authorising Officers are required to have a thorough understanding of section 9 of the Covert Surveillance and Property Interference code of practice (August 2018).

O ACQUISITION OF COMMUNICATIONS DATA

Background

1. The Investigatory Powers Act 2016 ('IPA') provides a mechanism for the Council to acquire communications data from telecommunications and postal operators by setting up an authorisation procedure. The definition of communications data is very wide and can include subscriber information, telephone numbers called or received, the IP address of the sender of an email or the status or contact details of the customer of a social networking site. However it does not include the content of the communications.

2. The legislation seeks to ensure that public authorities only acquire communications data where it is necessary and proportionate, for a legally prescribed purpose, and that the acquisition is carried out in such a way that the risk of infringing the human rights of individuals is kept to a minimum. For the Council the only legal purpose for acquiring communications data is for the preventing or detecting crime or of preventing disorder.

3. The Home Office has issued a Communications Data Code of Practice which can be found at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf .This policy must be read in conjunction with the Code of Practice and all staff involved in the acquisition of communications data must have regard to the provisions of the Code of Practice.

Introduction

4. The Council will on occasion need to acquire communications data to carry out its enforcement functions effectively. By following the authorisation procedures set out by IPA 2016, officers can demonstrate that the data acquisition is for a permitted purpose in connection with a specific investigation or operation and that it is a necessary and proportionate measure to take, given all the circumstances.

5. The purpose of this policy is to reinforce the requirements of the IPA 2016 and the Communications Data Code of Practice, to ensure compliance with the law, to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.

6. All communications data acquisition must be done in accordance with the legislative framework and this policy including where these activities are carried out by a contractor. Any restrictions on the type of communications data that the Council is authorised to access and the tests to be applied must be observed, and any acquisition must be properly authorised and recorded. Within the Council, a Senior Responsible Officer is appointed to oversee the process for the acquisition of communications data (presently this post is held by the Monitoring Officer). They are responsible for the implementation and effective operation of this policy.

7. All applications for the acquisition of communications data made by the Council will be considered by an independent body, The Office for Communications Data Authorisations (OCDA) who perform this function on behalf of the Investigatory Powers Commissioner.

Communications Data

8. Communications data is the “who”, “when”, “where” and “how” of a communication but does not include the content and under no circumstances can the content of a communication be obtained. The Council has no right to listen in to telephone conversations without permission or read post or electronic communications before they have been received.

9. However, the definition of Communications Data in the legislation is very broad and the Communications Data Code of Practice gives specific examples of what is included and excluded from the definition. It includes the way in which, and by what method, a person or thing 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, of the communication.

10. Communications Data can include the address to which a letter or parcel 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 from which the communication was made. It covers electronic communications, including internet access, internet telephony, instant messaging and the use of apps.

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

12. **Telecommunications Data**: All communications data held by a telecommunications operator, or obtainable from a telecommunications system fall into one of two categories:

- data about the entity: this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).This might include subscriber details or billing information including payment methods.

- data about the event: this data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time, such as itemised telephone calls or their duration, or the location of a device when it was used to send a communication.

13. Apart from events data the Council can obtain communications data to prevent and detect crime and prevent disorder. The only lawful purpose for which the Council can obtain events data is in relation to **"serious crime".** This means an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

14. The Council may not make an application that requires the processing or disclosure of internet connection records for any purpose.

15. **Postal Data**. A postal service is a service which includes one or more of collection, sorting, conveyance, distribution and delivery of postal items. Postal data may be:

- Anything comprised in or attached to a communication for the purpose of the service by which it is transmitted. This can include addresses or markings of the sender or recipient written on the outside of the postal item or online tracking.

- Data relating to the use made by a person of a postal service. This can include redirection services, price and postage class used, registered post or special/recorded delivery and parcel consignment records.

- Information held or obtained about persons who have used a communications service such as PO Box numbers even if no mail has ever been received

16. Postal data must however be related to a postal service and does not include data which may be held about a customer more generally.

Accessing Communications Data

17. The Council is party to a collaborative agreement with the National Anti-Fraud Network (NAFN) and uses the NAFN shared SPoC (Single Point of Contact) services for the acquisition of Communications Data. Applicants consult a NAFN SPoC throughout the application process and the SPoC will scrutinise the applications independently. All applications are made electronically using the NAFN secure portal.

18. There are 5 roles set out within the Code of Practice in respect of who will be involved in the acquisition of communications data.

The Applicant

19. This is the person involved in conducting or assisting an investigation or operation within the Council who makes an application in writing

(electronically) for the acquisition of communications data. The Council limits the persons who are permitted to make an application to acquire communications data to those who have had sufficient training and knowledge of this area of law and only Authorised Officers may submit an application.

The Single Point of Contact (SPoC)

20. The SPoC promotes efficiency and good practices in ensuring that only practical and lawful applications for communications data are made.

21. Applicants follow the advice of the SPoC to ensure that the Council acts in a lawful and informed manner.

22. No application is submitted for authorisation until the SPoC is satisfied that it practical and lawful and that the appropriate verification procedure has been followed by the Council.

The Authorising Individual

23. Communications data applications can be authorised by three separate categories of individual depending on the circumstances of the specific case.

- An authorising officer in the Office for Communications Data Authorisations.
- The designated senior officer who holds a prescribed office or rank in the Council (where the independent authorisation does not apply)..
- A judicial commissioner who is responsible for approving requests to identify or confirm journalistic sources.

The Senior Responsible Officer

24. The Senior Responsible Officer is responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- engagement with authorising officers in the Office for Communications Data Authorisations (where relevant);
- compliance with Part 3 of the IPA and with the Communications Data Code of Practice, including responsibility for novel and contentious cases;
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications submitted to OCDA by the public authority;
- engagement with the IPC's inspectors when they conduct their inspections;
- where necessary, oversight of the implementation of post inspection action plans approved by the IPC. Within the Council, the Senior Responsible Officer is the Monitoring Officer.

The Application Process

25. The Applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data. This is done via the NAFN secure portal by completing the electronic application form. The applicant will have regard to the Communications Data Code of Practice in completing this form and in particular:

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under IPA;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- include the operation name (if applicable) to which the application relates
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- consider and, where appropriate, describe any meaningful collateral intrusion
- the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

Necessity

26. The Applicant must ensure that any application is necessary for the purpose of preventing or detecting crime or preventing disorder. In addition events data must only be sought for serious crime. See paragraph 13 above. The application should demonstrate how the investigation, the person and the communications data link together for the statutory purpose specified. Further detail on necessity is provided in the Communications Data Code of Practice.

Proportionality

27. The Applicant must also ensure that the application is proportionate to what is sought to be achieved by obtaining the specified communications data and that the conduct is no more than is required in the circumstances. This involves balancing the interference with an individual's rights and freedoms against a specific benefit to an investigation or operation and that it is in the public interest. In particular the Council must consider:

- whether what is sought to be achieved could be reasonably achieved by other less intrusive means
- whether the level of protection to be applied should be higher because of the sensitivity of the information
- the public interest in the integrity of the postal or telecommunications system
- any other aspects of the public interest in the protection of privacy.
- Collateral Intrusion. When accessing communications data there is the potential to obtain information relating to individuals who are not the subject of the investigation. Therefore the degree of collateral intrusion must be considered particularly when applying for events data. Taking all things together it may be that an interference with the rights of an individual may still not be justified because the adverse impact on another individual or group is too severe. The relevance of the data being sought and how it will benefit the investigation should be demonstrated. Any time periods must be explained outlining how these are proportionate to the event under investigation.
- Overall a consideration should be given to the rights of the individual and balancing these rights against the benefit of to the investigation. Further detail on proportionality is given in the Communications Data Code of Practice.

28. The application form will be reviewed by the National Anti-Fraud Network (NAFN) SPoC. If changes need to be made it will be referred back to the Applicant with suggestions, otherwise the NAFN SPoC will complete the relevant part and forward it to the Local Authority Verifier.

29. Local Authority Verifier will confirm to the SPoC that they have been notified of the application via the NAFN electronic portal.

30. When satisfied that the Council has completed the verification process the NAFN SPoC will forward the application to the Office for Communications Data for consideration by an Authoriser. The application will only be authorised if the officer is satisfied that the acquisition of communications data meets the requirements and is necessary and proportionate in the circumstances.

31. An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month.

32. In the event that the application is rejected the Council may decide to discontinue with the application, amend the application, or ask for a review of the decision. A review of the decision can only be requested with permission of the Senior Responsible Officer and will be instigated following the OCDA procedure.

33. An authorisation may authorise the NAFN SPoC to obtain the specific communications data, or to give notice to require a telecommunications operator to obtain and disclose the specific data if it is not already in their

possession. The NAFN SPoC will proceed with the acquisition of communications data from the service provider on behalf of the Council in accordance with the authorisation.

34. Any valid authorisation may be renewed for up to a period of one month by the grant of a further authorisation. The applicant should prepare an addendum to the original application explaining why there is a continuing requirement to acquire data and again demonstrating that it is necessary and proportionate in the circumstances. A renewed authorisation takes effect upon the expiry of the original authorisation.

35. Where the Applicant identifies that a granted authorisation is no longer necessary for the statutory purpose or it is no longer proportionate it must be cancelled by notifying the NAFN SPoC. They will cease the authorised conduct and ensure that any notices are cancelled by advising the telecommunications operator and the authorising individual who will produce a record of the notice being cancelled.

Data Protection

36. Communications data obtained by the Council can only be held for the statutory purpose of preventing or detecting crime or of preventing disorder and should be adequate, relevant and not excessive for this purpose. In addition the specific requirements of data protection legislation should be adhered to.

37. Communications data held by the Council is classified marked 'OFFICIAL – SENSITIVE [LEGAL]' and only authorised personnel can have access to the material. Those persons are limited to the officers directly involved in the investigation of the specific case and those involved in the approval process.

38. Each Council enforcement team must ensure it has a secure, restricted access, electronic storage facility which is used for this purpose – being a prerequisite for making an application.

39. All material must be handled in accordance with Data Protection principles and all records should be securely destroyed as soon as they are no longer needed for any of the authorised purposes.

40. Any additional disclosure of data must be in accordance with the provisions of data protection legislation.

41. The Council must keep a detailed record of all applications, authorisations, notices, renewals and cancellations so that they are available for inspection by the Investigatory Powers Commissioner or to allow the Investigatory Powers tribunal to carry out its functions. NAFN complies with these requirements on the Council's behalf.

42. Where authorised conduct results in the acquisition of excess data, or its disclosure by a telecommunications operator or postal operator in order to comply with the requirement of a notice, the excess data acquired or

disclosed should only be retained by the Council where appropriate to do so – for example in relation to a criminal investigation.

43. The Council is responsible for the retention of records to comply with the statutory obligations of the Criminal Procedure and Investigations Act 1996. There is a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed

44. If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The senior responsible officer will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation

Errors

45. Proper application of IPA and Code of Practice in line with this policy including the careful preparation and checking of applications, and authorisations, should reduce the scope for making errors. However NAFN keep a records of any errors that have occurred and a report and explanation is sent by NAFN's Senior Responsible officer to the Commissioner as soon as is practicable.

Complaints

46. The Council has a complaints procedure which can be accessed here https://www.merton.gov.uk/council-and-local-democracy/complaints-compliments-and-comments . In addition the Investigatory Powers Tribunal has power to investigate claims or complaints from anyone who believes they have been a victim of unlawful action by a public authority using covert investigative techniques.

Oversight

47. The Senior Responsible officer shall establish and maintain regular meetings, as appropriate, to check and test processes and address any training requirements.

48. The SRO shall record any issues arising from these meetings or the process as it operates in practice and determine any actions necessary to ensure the proper application of this policy.

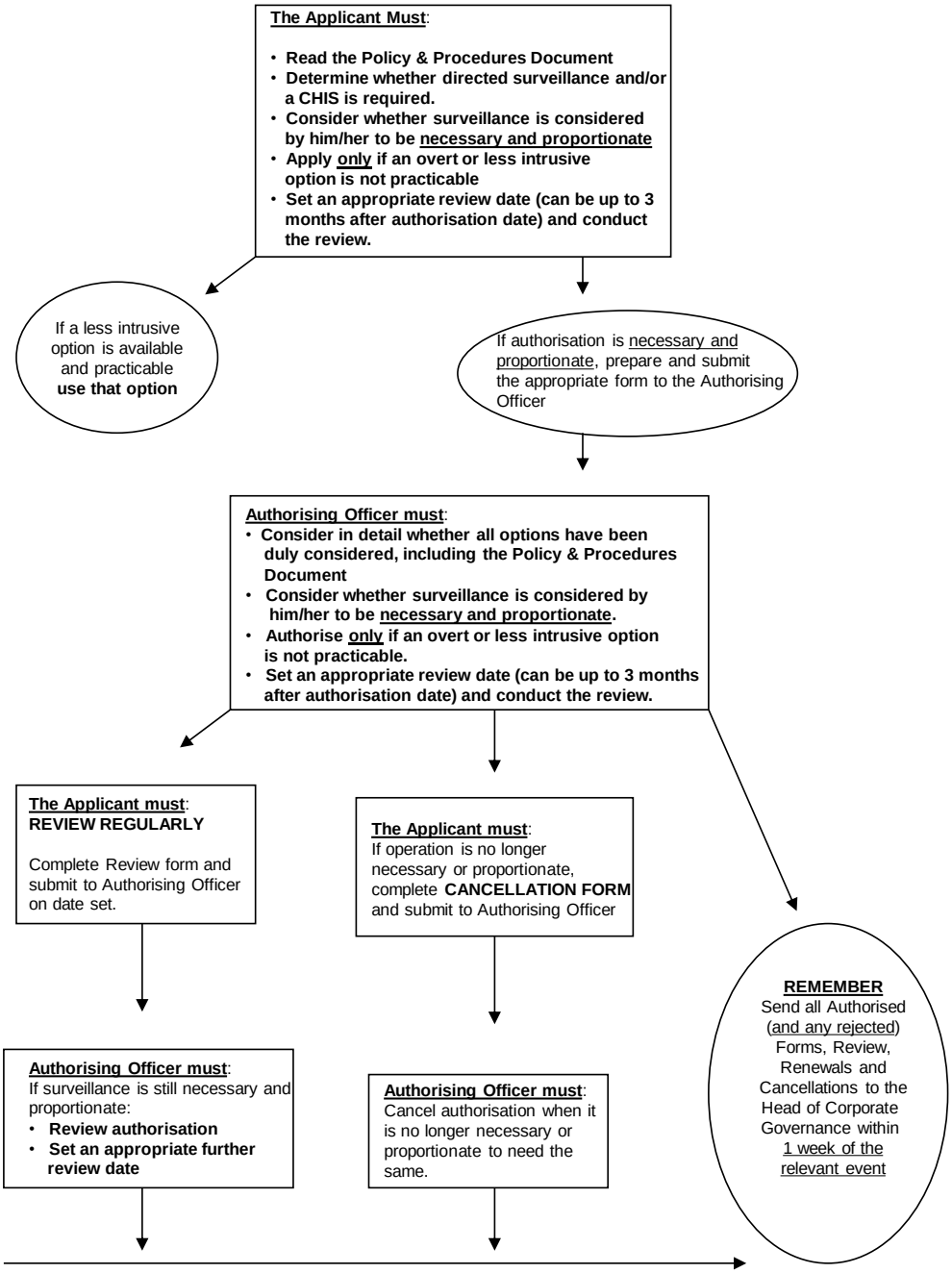
49. In addition the SRO shall arrange an oversight meeting as soon as possible following an inspection to discuss issues and outcomes as appropriate.

Review

50. This policy will be reviewed annually or sooner if legislation changes.

APPENDIX 1

RIPA FLOW CHART- Directed Surveillance and CHIS



Appendix 2

Direct Surveillance Forms

These forms may be downloaded from http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

Application **http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc**

Renewal **https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance**

Review **https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance**

Cancellation **https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form**

Appendix 3

CHIS Forms

These forms may be downloaded from http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

Application **http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application**

Renewal **http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal**

Review **http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review**

Cancellation **http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation**

USE OF COVERT SURVEILLANCE EQUIPTMENT - Technical Guidance

1. Introduction

The use of covert CCTV systems across the London Borough of Merton is governed by law and policy. The Enforcement and Inspection Team EOI has to comply with the provisions of the Data Protection Act 2018 , the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000. Compliance with these Acts, their associated Codes of Practice and the council's RIPA Policy will assist the users of the surveillance equipment in meeting their legal obligations.

2. Initial Assessment Procedures

Before installing and using covert surveillance equipment users will need to ENSURE authorisation to install surveillance had been obtained and establish the purpose or purposes for which they intend to use the equipment, as the First Data Protection Principle requires Data Controllers to have a legitimate basis for processing personal data, in this case images of individuals. Hence the following procedures should be carried out:

1. Assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment and document this process.
2. Establish the purpose of the operation.
3. Establish the person or persons responsible for ensuring the day-to-day compliance with this Code of Practice.
4. Establish the associated security and disclosure policies.
5. Obtain the approval of the Authorising Officer for this activity by using the specified forms and processes set out in the RIPA Policy.

Equipment

The team currently has access to 5 surveillance systems. The system consist of 22 bullet cameras of varying sizes, x 3- 35mm zoom cameras and 18 hard disc cartridges of varying sizes. All the equipment is kept in a locked cupboard and can only be accessed by key, which is managed by a diary. All equipment being removed MUST be logged out in the dairy.

3. Deploying the Systems/cameras

1. The equipment should be sited in such a way that it monitors only the area intended, i.e. where the incident of fly-tipping is likely to occur.
2. The user/s should only use the covert system/s as set out in the authorisation document.
3. Investigating officers must be aware of the purpose(s) for which the operation has been established.

4. Investigating officers are expected to fill in the appropriate risk assessment and premises consent forms when necessary.

4. Handling of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. The following standards should therefore be observed:

1. Carry out an initial check on installation to ensure that the equipment performs properly.
2. Ensure that, where tapes are used they are of good quality.
3. Images should be retained until prosecution is completed.
4. ALL storage discs must be kept in the metal locked cupboard except in the case of viewing, production as evidence of court proceeding.
5. Media should not continue to be used once it becomes clear that the quality of the images has begun to deteriorate.
6. All systems and cameras should be properly maintained and serviced to ensure that clear images are recorded and a maintenance log kept.
7. Cameras should be protected from vandalism in order to ensure that they remain in working order.

5. Processing the Images

To maintain the integrity of the images and to protect the rights of the individual, the following standards should be maintained:

1. Access to recorded images should be restricted to the person responsible for managing the investigation (the Data Owner) or their nominee who will decide whether to allow requests for access by third parties.
2. Where images are retained, it is essential that their integrity be maintained, whether to ensure their evidential value or to protect the rights of the people whose images may have been recorded.
3. Images should not be retained for longer than is necessary; once the retention period has expired, the images should be removed or erased. If in doubt. Speak to the Information Governance Team or Legal Services.
4. If the images are retained for evidential purposes, they should be kept in a secure place (locked metal cupboard) to which access is controlled.
5. On removing the medium on which images have been recorded for use in legal proceedings, the operator should ensure that s/he has documented the date on which the images were removed from the general system for such use, the reason for doing so, any crime incident number to which the images may be relevant, the new location of the images and the signature of the

person collecting the images. In such instances this will only be officer from the Metropolitan Police or an authorised officer within the Council.

6. Access to and Disclosure of Images to Third Parties

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of the individual are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Staff should maintain the following standards:

1. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the recording equipment.

2. All access to the medium on which images are recorded should be documented.

3. Disclosure of recorded images to third parties, whether officers of the Enforcement Team or not, should only be made in limited and prescribed circumstances.

4. All requests for access or for disclosure should be recorded and, if access is denied, the reason should be documented.

5. If access to or disclosure of images is allowed, then the following should be recorded:

    - The date and time access was allowed or disclosure made.

    - The identification of any third party who was allowed access or to whom disclosure was made.

    - The reason for allowing access or disclosure.

    - The extent of the information to which access was allowed or which was disclosed.

8. Monitoring Compliance with this Code of Practice

1. The Enforcement and Inspection Manager will undertake regular reviews of the documented procedures and the above processes to ensure that the provisions of this Code are being complied with.