LONDON BOROUGH OF MERTON

POLICY & PROCEDURE

Regulation of Investigatory Powers act 2000 (RIPA)

London Borough of Merton
Policy date: 2010
Revised and updated: July 2016

CONTENTS

Acknowledgement: The London Borough of Merton is grateful to Birmingham City Council whose Policy and Procedure in this area has been most helpful and is adapted in this document.

A INTRODUCTION

1. OBJECTIVE: SUSTAINABLE COMMUNITIES; SAFER AND STRONGER COMMUNITIES

Merton 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 Merton to carry out enforcement functions to take full action against those who flout the law. Merton 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), benefit 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.

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 December 2014, 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

B AUTHORISING OFFICER RESPONSIBILITIES

1. Local authorities will only be able to conduct directed surveillance under RIPA where the 'crime threshold' is satisfied (subject to exceptions) and judicial approval has been granted for the operation

2. It is essential that Chief Officers of the Council and Authorising Officers in their Departments, take personal responsibility for the effective and efficient observance of this document. It shall be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained as 'Applicants'.

3. Authorising Officers will also ensure that staff who report to them follow this Policy and Procedures Document and do not undertake or carry out any form of covert surveillance without first obtaining the relevant authorisations in compliance with this document.

4. 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 s/he is 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.

5. If an Authorising Officer is in any doubt, s/he should obtain prior guidance from his/her Chief Officer, the Council's Health & Safety Officer and/or the Assistant Director Corporate Governance. However, there is no sign-off or authorisation required other than by the Authorising Officer.

6. Authorising Officers must also ensure that, when sending copies of Forms to the Assistant Director Corporate Governance (or any other relevant authority), the forms are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.

7. In Accordance with SI 2010 521, the Senior Responsible Officer with responsibility for Authorising Officers is the Assistant Director Corporate Governance. The Assistant Director Corporate Governance has delegated powers to appoint Authorising Officers. Authorising Officers will only be appointed if the Assistant Director Corporate Governance is satisfied that they have received suitable training on RIPA.

8. The Assistant Director Corporate Governance will review this policy periodically and annual reports on performance of the policy will be presented to the Standards Committee of the Council.

9. Quarterly reports on the use of RIPA will 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;
   (a) necessary (as defined in this document); and
   (b) 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 'covert human intelligence source' ('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 and to the paragraph 2 on Authorising Officers.
5. If the correct procedures are not followed, evidence may be disallowed by the courts, 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, s/he should ask the Assistant Director Corporate Governance 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 (eg. 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; and
- is not intrusive surveillance
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act reasonable, eg. spotting something suspicious and continuing to observe it; and

- it is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) RIPA).*

7. *Private Information* in relation to a person includes any information relating to his private and family life, his home or his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others with whom s/he comes into contact.

8. 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.

9. 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 his/her business may also reveal information about his or her private life and the private lives of others.

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

11. Only officers authorised by the Assistant Director Corporate Governance as Authorising Officers for the purpose of RIPA may authorise directed surveillance'

12. *Intrusive Surveillance*

This is when it:-

- is covert;
- relates to residential premises and private vehicles, even if used on a temporary basis. This includes the use of tracking devices on vehicles; and
- involves the presence of a person in the premises or in the vehicle 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.

13. **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. Council officers may not carry out intrusive surveillance.

14. "**Necessity**"
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?

15. 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' set out in regulation 7A of the 2010 Order.

The 'crime threshold' is met if the purpose of the directed surveillance is to detect or prevent criminal offences for which the punishment on conviction is a term of imprisonment of not less than 6 months or the offences 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.

16. Proportionality

Proportionality encapsulates three concepts:-

- the surveillance should not be excessive in relation to the gravity of the offence being investigated;
- the least intrusive method of surveillance should be chosen; and
- collateral intrusion, the invasion of third parties' privacy, should, so far as possible, be minimised.

17. Proportionality involves balancing the intrusiveness of the activity on the target subject and the others who might be affected by it, against the need for

the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances (each case will be judged on its merits) or if the information which is sought could be 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.

18. Collateral Intrusion

Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

19. 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.

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

It is unlikely that a Local Authority will want to use a CHIS. If it appears that use of a CHIS may be required Authorising Officers must seek legal advice from the Assistant Director Corporate Governance.

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.

2. 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.

3. However, by virtue of section 26(8) (c) of the Act, 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. It is recommended that legal advice 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.

Juvenile Sources

6. 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 his or her absence, a Chief Officer can authorise the use of a juvenile as a source.

Vulnerable Individuals

7. 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.

8. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive, or in his or her 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 Assistant Director Corporate Governance.

Anti-Social Behaviour Activities (eg. Noise, Violence, Race 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. Recording the level of noise (eg. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

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.

G 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.

   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 Assistant Director Corporate Governance. Officers can only be Authorising Officers if they are the Chief Executive, Chief Officers, Heads of Service, or other Level 3 Unit Managers who are considered to be suitable by the Assistant Director Corporate Governance. Appointments of these officers are subject to the training requirements set out in paragraph 4 below.
3. Graham – Is 'Level 3' manager a current term? If so, is John Hillarby Level 3? He reports to Paul Foster who reports to John Hill? If so, it may imply John Hillarby is not eligible to be an Authorised Officer (despite being the most qualified person to hold such a position).

4. 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. **The authorisations do not lapse with time.**

Training Records

5. The Assistant Director Corporate Governance will only appoint Authorising Officers if satisfied that they have undertaken suitable training on RIPA. The Assistant Director Corporate Governance will usually expect that evidence of suitable training to be supplied in the form of a certificate from the relevant Chief Officer to the effect that the Authorising Officer has completed a suitable course of instruction.

6. The Assistant Director Corporate Governance will maintain a Register of Authorising Officers and details of training undertaken by them.

7. If the Assistant Director Corporate Governance is of the view that an Authorising Officer has not complied fully with the requirements of this document, or the training provided to him, the Assistant Director Corporate Governance is duly authorised to withdraw that Officer's authorisation until s/he has undertaken further approved training or has attended a one-to-one meeting with the Assistant Director Corporate Governance.

Application Forms

8. Only the approved RIPA forms set out in this document must be used. The forms are also on the Intranet.

9. '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

10. '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

11. 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

12. 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 the 2000 Act;
- 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.

13. Before an Authorising Officer signs a Form, s/he must:-

(a) Be mindful of this Policy & Procedures document and the training s/he has undertaken

(b) Satisfy his/herself that the RIPA authorisation is:-

(i) in accordance with the law**;**
(ii) that the offence being investigated satisfies the crime threshold test).;
(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) Set a date for review of the authorisation and review on only that date;

(f) Obtain a Unique Reference Number (URN) for the application from the Information Governance Team on 020 8545 4182

(g) Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Assistant Director of Corporate Governance, Central Register, within 5 days of the relevant authorisation, review, renewal, cancellation or rejection**.**

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

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

(i) Allocate a Unique Reference Number (URN) for each form:-
Year / Department / Number of Application;

(j) Ensure that any RIPA Central Register is duly completed, and that a copy of the RIPA forms (and any review / renewal / cancellation of the same) is forwarded to the Assistant Director of Corporate Governance, within 5 days (Graham – (as was) paragraph 12(g) cites “5 days” rather than “1 week” – it would be better to be consistent) of the relevant authorisation, review, renewal, cancellation or rejection;

(k) In the case of notices relating to communications data, these will be kept by a ‘Designated Person’ selected by the Assistant Director of

Corporate Governance,. The Assistant Director of Corporate Governance shall have access to such forms and as when required;

(l) If unsure on any matter, authorising officers should obtain advice from the Assistant Director of Corporate Governance, before signing any forms.

Additional Safeguards when Authorising a CHIS

15. 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 his 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. It is strongly recommended that legal advice is obtained in relation to the authorisation of a CHIS.

16. Approval by a Justice of the Peace (JP)
Judicial approval is required before acting on the authorisation to carry out directed surveillance; conduct or use of a CHIS; or obtaining communications data.

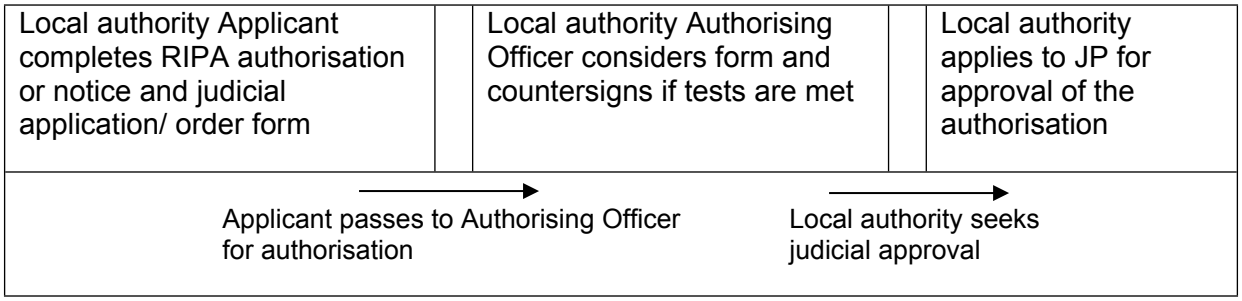
17. Judicial approval in also required on the renewal of an authorisation.

18. The JP must decide whether the grant or renewal of an authorisation to use RIPA 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, CHIS and communications data) at the same time,

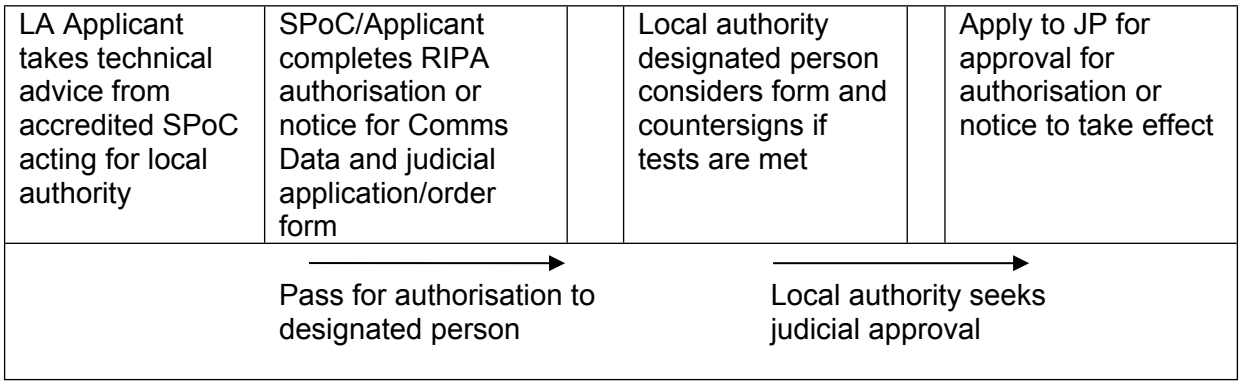
in practice, it is better to separate the applications for approval as different considerations apply to these different techniques, this may prove be difficult to perform with the degree of clarity required. It is recommended that separate authorisations or notices to use different RIPA techniques should be submitted.

19. Please note that the application and any renewal of the application require magistrates' 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)



Communications Data



20. The Role of the JP

The role of the JP is set out in section 23A RIPA (for Communications Data) and section 32A RIPA (for directed surveillance and CHIS).

21. The Act provides that the authorisation, or in the case of communications data, the notice, shall not take effect until the JP has made an order approving such an authorisation or notice. 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 or notice was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter;

- in the case of a CHIS authorisation, that there 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 2000[3] 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 or in the case of communications data, notice was not in breach of any restriction imposed by virtue of an order made under the following sections of section 25(3) RIPA(for communications data),

Urgent Authorisations

22. Because an authorisation under RIPA requires judicial approval urgent oral authorisations are no longer permitted.

Duration

23. 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).

24. Notices/Authorities issued under s22 compelling disclosure of Communications Data are only valid for one month, but can be renewed for subsequent periods of month, at any time.

25. 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.

26. 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.

27. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours.

H 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 (as per normal procedure) 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 (eg. Police, HMRC etc):-

    (a) wishes to use the Council's resources (eg. 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 Assistant Director of Corporate Governance 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) wish 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 not 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 before 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 Assistant Director Corporate Governance at the earliest opportunity.**

I. DIRECTED SURVEILLANCE - SOCIAL MEDIA POLICY

Background

1. The growth of social media usage has increased the volume of personal information available online covering such details as an individual's employment, friends and personal life.

2. The Chief Surveillance Commissioner has identified that public authorities might be

> *"tempted to conduct on line investigations from a desktop, as this saves time and money, and often provides far more detail about someone's personal lifestyle, employment, associates, etc. But just because one can, does not mean one should. The same considerations of privacy, and especially collateral intrusion against innocent parties, must be applied regardless of the technological advances."* *(Annual Report 2013/14)*

3. The Office of the Surveillance Commissioner advises that gathering intelligence and data through repeated viewing of the internet should be considered within the context of the protection that RIPA provides.

4. If you are considering monitoring social media such as Facebook in connection with an investigation you should first seek advice on whether RIPA authorisation is needed.

5. There may be situations where individuals publish information freely using Twitter accounts or LinkedIn profiles if so there is unlikely to be any interference with an individual's right to privacy as provided for by Article 8 of the Human Rights Act). This is also likely to be the case with other information published openly on the Internet.

6. Even if the user has not used privacy settings to restrict access, this does not necessarily mean that they have made a decision to publish personal information to the world.

7. In the event that your proposed use of social media in connection with an investigation amounts to covert directed surveillance within the scope of RIPA by electronic means, a RIPA authorisation for directed surveillance will be required. It should be noted that it is likely to be proportionate, in connection with an investigation (e.g. benefit fraud), to make a single visit to an unsecured Facebook profile. Further visits could amount to surveillance.

8. Merton's policy in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

   • The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance.

   • Whenever you intend to use the internet as part of an investigation, you must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights. As a rule, directed surveillance should be the choice of last resort.

   • Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case.

   • Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.

   • Officers must not "friend" individuals on social networks

   • Officers must not use their own private accounts to view the social networking accounts of other individuals.

   • Officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation

   • Further viewing of open profiles on social media networking sites to gather evidence or to monitor an individuals status must only take place once a RIPA Authorisation has been granted and approved by a JP

   • 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.

Non RIPA Activity.

9. It has been acknowledged that there may be occasions when during the course of an investigation that it may become necessary to conduct

surveillance of individuals in respect of matters that do not satisfy the crime threshold.

10. In these circumstances, the Office of the Surveillance Commissioner ('the OSC') has stated that it would be "good practice" for the investigating officer to go through the RIPA authorisation process in terms of:-

    i. Why there is no other alternative to undertaking the directed surveillance
    ii. Why the surveillance is necessary; and
    iii. How it is proportionate in the circumstances.

11. 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.

Test purchase exercises

12. 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.

J 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 Assistant Director Corporate Governance.**

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 Assistant Director Corporate Governance

3. Authorising Officers must forward a copy of the form to the Assistant Director Corporate Governance for the Central Register, within 5 days of the authorisation, review, renewal, cancellation or rejection. The Assistant Director Corporate Governance 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.

8. The Council shall retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

5. The Office of the Surveillance Commissioners 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 Assistant Director Corporate Governance to respond to such communications.

K ACQUISITION OF COMMUNICATIONS DATA

What is Communications Data?

1. Communications data means any traffic or any information that is or has been sent by or over a telecommunications system or postal system, together with information about the use of the system made by any person.

Powers

2. There are two powers granted by s22 RIPA in respect of the acquisition of communications data from telecommunications and postal companies (the Communications Service Provider) – s22(3) and s22(4).

3. s22 (3) provides that an Authorising Officer can authorise another person within the same local authority to collect the data. This allows Merton as a local authority to collect the communications data themselves i.e. if a communications service provider is unable to collect the data, an authorisation under this section would permit Merton to collect the communications data itself.

4. Under s22 (4) an Authorising Officer may serve a notice to compel a communications service provider to obtain and disclose, or just disclose communications data in their possession. The only ground on which Merton may permit the issuing of a s22 notice is **to prevent or detect crime or prevent disorder.**

5. The appropriate form should be used when the communications service provider is being required to disclose or obtain and disclose the specified information.

7. Once issued the notice must be sent to the communications service provider. In issuing a notice, the Authorising Officer can authorise another person to liaise with the communications service provider covered by the notice.

9. Authorising Officers may sign the forms for the acquisition of communications data. These forms will be retained by the Single Point of Contact (SPoC) as part of a record of compliance with the relevant provisions.

Who does what

There are four different roles that are involved in the authorisation of applications.

Applicant

10. The Applicant will be an officer who is involved in the investigation or operation for the council and who will make the written application for the acquisition of communications data. The Applicant will set out the necessity and proportionality of the need to obtain the communications data.

Designated Person (also known as Authorising Officer)

11. The designated person is also known as the Authorising Officer. They will consider the application and decide whether the acquisition of communications data is necessary and proportionate. If they believe it is, they will authorise the application or give a notice.

12. The Authorising Officer will assess the need to acquire or obtain communications data taking account of any advice provided by the single point of contact (SPoC).

13. The Authorising Officer must be independent from operations and investigations when granting authorisations or giving notices related to those operations.

Single Point of Contact

14. The role of the single point of contact (SPoC) is to maintain effective co-operation between the council and communications service providers in the lawful acquisition and disclosure of communications data.

15. To be a SPoC the officer must undertake specialist training recognised by the Home Office and register his or her details with the Home Office. A Register of the council's SPoCs is held by the Assistant Director Corporate Governance together with details of the training undertaken.

16. The SPoC will:

- assess whether access to communications data is reasonably practical for the postal or telecommunications operator;
- advise Applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators
- advise Applicants and Authorising Officers on whether communications data falls under section 21(4)(a), (b) or (c) of RIPA
- provide safeguards for authentication
- assess any cost and resource implications to both the council and postal or telecommunications operator.

Senior Responsible Officer

17. Each council must have a Senior Responsible Officer who will:

- ensure there is a proper process in place in the council to acquire communications data;
- ensure compliance with Chapter II of Part 1 of RIPA and with the relevant Codes of Practice;

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

- ensure that any errors are reported to the Interception of Communications Commissioner's Office (IOCCO), including the cause of errors and remedial action to minimise any repetition;
- meet the IOCCO inspectors when they conduct their inspections and;
- oversee the implementation of post –inspection action plans approved by the Commissioner.

18. Merton Council's Senior Responsible Officer is the Assistant Director Corporate Governance.

19. Merton uses the National Anti Fraud Network (NAFN) system to make applications for communications data. NAFN is government funded organisation providing data and intelligence services. It provides the SPoC for applications and access to a secure online system. The system takes the Applicant through the process and offers online guidance.

Application Forms

20. The system contains the forms the Applicant must complete in order to progress the application to completion. It allows the Applicant to submit and receive approval online and to track progress.

Procedure

21. All applications to obtain communications data must be channelled through the NAFN SPoC. In considering making an application to obtain communications data the Applicant should contact the SPoC for advice.

22. In completing the application the Applicant must address the issues of necessity, proportionality and collateral intrusion as contained in the Acquisition and Disclosure of Communications Data Code of Practice (2015)

Necessity

The Applicant should consider the necessity of obtaining communications data by addressing three points
The event under investigation, such as a crime
the person, such as a suspect, and how they are linked to the event; and
the communications data, such as a telephone number or IP address and how this is linked to the person and the event.

The Applicant should explain the event, the person and the communications data and how these three are linked. The link must be established to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Proportionality

The application should explain how obtaining the data will benefit the investigation or operation. It should explain how the benefit of obtaining the data justifies the level of intrusion and confirm that other less intrusive investigations have already been undertaken where possible. Any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation.

The application should also consider the rights (to privacy and, in relevant cases, freedom of expression) of the individual and balance these rights against the benefit to the investigation.

"Collateral intrusion is the obtaining of any information relating to individuals other than the subject(s) of the investigation." The application should identify the details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. If no collateral intrusion risk is identified such absence should be noted.

"Unintended consequences of an application are outcomes that are not intended by the application." These are more likely to occur in more complicated requests for traffic data or in applications for the data of those in professions with duties of confidentiality. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered.

23. The Applicant will log in and complete the required fields in the NAFN system.

24. The Applicant will submit the completed fields to the NAFN SPoC who will check whether the application can go forward for authorisation.

25. When checked the application will be routed to the Authorising Officer for authorisation. The Authorising Officer must be someone in the council who is independent from the operation and investigation to be undertaken when granting authorisation or giving notices related to those operations.

26. The Authorising Officer will consider:

(a) whether the case justifies the accessing of communications data for the **purposes of preventing or detecting crime or of preventing disorder** and why obtaining the data is **necessary;** and

(b) whether obtaining access to the data by the conduct authorised, or required of the postal or telecommunications operator in the case of a notice, is **proportionate** to what is sought to be achieved.

27. The Authorising Officer will complete the application as required on the NAFN system.

28. Within the NAFN system, when the application is authorised, the paperwork required for the magistrate's hearing will be generated.

29. Upon authorisation, the Applicant should contact the court to arrange a suitable hearing date. The Applicant will attend court.

30. If the application is approved by the court the Authorising Officer will sign the Notice to the Communication Service Provider, complete the date/time of issue and pass to the SPoC. If the SPoC is satisfied that the application should proceed, the SPoC will then issue the Notice to the Communications service provider and

Duration

31. Authorisations and notices are only valid for one month. A shorter period should be specified if this is satisfied by the request. To renew an authorisation or notice during the month the Applicant must follow the same procedure as obtaining a fresh authorisation or notice.

32. An Authorising Officer must cancel an authorisation or notice as soon as it is no longer necessary or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the Authorising Officer who issued it.

Record Management

33. Applications, authorisations and notices for communications data must be retained by the SPoC until audited by the IOCCO. All such documentation must be kept in locked storage.

Errors

34. Where any errors have occurred in the granting of authorisations or the giving of notices, a record shall be kept and a report and explanation sent to the IOCCO as soon as reasonably practicable.

Oversight

35. The IOCCO will write to the council from time to time requesting information as to the numbers of applications for communications data and confirmation as to whether there have been any errors which have occurred when obtaining data communications. It will be the responsibility of the Assistant Director Corporate Governance to respond to such communications with the assistance of the SPoC.

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

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

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

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**

Appendix 4 Accessing Communications Data

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/communications-data1.doc**

Notice **http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/RIPAschedule-for-subscriber-info**

Log Sheet **Please contact the SPoC**

Cancellation **Please contact the SPoC**

Reporting an error to the Interception of Communications Commissioner's Office
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/reporting-public-authority-error

Appendix 5

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 1998, 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. There are only 3 persons in the London Borough Of Merton who can authorise surveillance operations. Helen Catling – Transport, Ian Murrell-Trading Standards and Chris Johnson-Internal Audit.

3. 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 flytiipping 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 his/her 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.

This page is intentionally left blank