THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Operational policy and guidance for the use of covert surveillance and "covert human intelligence sources"

Version No.	Author	Date
		August 2023

CONTENTS

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory framework under which covert surveillance and use of covert human intelligence sources can be authorised and activity conducted compatibly with the Human Rights Act 1998.

1.2 It provides a framework for the council to obtain authorisation from designated authorising officers on statutory grounds of necessity and proportionality. The process exhibits and records the respect for privacy and the framework ensures compliance.

1.3 Failure to obtain authorisation in accordance with RIPA does not in itself amount to unlawful activity; however, if the authority is challenged by way of defence to either a case brought, or a challenge to the way surveillance was carried out, it will be difficult to justify that the activity is in accordance with the law without a RIPA authorisation.

RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

1.4 In addition to the legislation itself, the Home Office has issued Codes of Practice dealing with covert surveillance and covert human intelligence sources – see https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice.

This guide is designed to cover the aspects of RIPA that regulate the use of investigatory powers by the Council.

2. What does RIPA do?

2.1 RIPA regulates the use of covert surveillance and "covert human intelligence sources". A covert human intelligence source is someone who uses a relationship with a third party in a secretive manner to obtain or give information – for instance someone working "under cover". This operational guidance covers these aspects of the Act.

3. Some definitions

"*Covert"*: Concealed, done secretly

"Covert surveillance": Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

"*Directed surveillance*": Surveillance which is covert, but not intrusive, and is undertaken for the purposes of a specific investigation or specific operation, in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) and otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the Act to be sought for the carrying out of the surveillance. An example might be where a police officer on patrol sees a person acting suspiciously and decides to watch them surreptitiously to see whether they are intending to commit a crime.

"*Intrusive surveillance*": Is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. **The council is not permitted to authorise and undertake intrusive surveillance under RIPA.**

"Private information": Includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

"*Confidential Information":* Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material.

4. RIPA and Surveillance – what is not covered

4.1 General observation forms part of the duties of some council officers. They may, for instance, be on duty at events in the City and will monitor the crowd to maintain public safety and prevent disorder. This activity is unlikely to be regulated by RIPA.

4.2 Neither do the provisions of the Act cover the use of covert CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. There may, however, be occasions where public authorities use material obtained from overt CCTV systems for the purpose of specific investigation or operation, in such cases authorisation for direct surveillance may be necessary.

5. RIPA and Surveillance – What is covered?

5.1 The Act is designed to regulate the use of "covert" surveillance. A surveillance operation might obtain private information about a person, the authorisation

procedures set out in this operational guidance should be followed and the surveillance treated as being “directed”.

5.2 What is “directed surveillance”?

5.2.1 The monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications where this is done in a manner calculated to ensure that the subject of surveillance is unaware that they are being monitored or observed etc.

5.2.2 The recording of anything monitored observed or listened to during surveillance.

5.2.3 Use of a surveillance device, e.g. a hidden video camera, a listening device.

5.2.4 Directed surveillance is covert surveillance that is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any persons. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance. e.g. a plain clothes police officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol.

5.2.5 Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. This activity is defined as "intrusive surveillance" and the council cannot do it (see paragraph 6).

5.2.6 In practice, the sort of directed surveillance which the council might conduct includes the use of concealed cameras as part of an investigation into antisocial behaviour or breach of tenancy conditions. It might include covert surveillance connected with the enforcement of environmental health or planning regulations or in connection with investigating benefit fraud. You should treat anything involving the use of concealed cameras or anything involving keeping covert observation on premises or people as potentially amounting to directed surveillance which may require authorisation in accordance with RIPA.

5.2.7 If you are unsure, please take advice either from your manager or supervisor, or from the Director, Law and Governance. If the proposed activity is covert surveillance likely to interfere with privacy, but does not fulfil all of the criteria to require RIPA authorisation, then seek advice before undertaking such activity, since the interference with privacy will need to be justified.

5.2.8 Directed surveillance **must** be properly authorised in accordance with the procedure set out in section 9. Failure to do so could leave the council vulnerable to legal action.

6. What is intrusive surveillance?

An important warning: the Council cannot authorise intrusive surveillance.

6.1 Intrusive surveillance is defined as covert surveillance that:

a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

6.2 In essence, intrusive surveillance amounts to intrusion into people's homes or vehicles either physically or by means of a surveillance device.

6.3 **Intrusive surveillance cannot be undertaken without authorisation and the Council cannot authorise intrusive surveillance.** Law enforcement and other similar organisations can authorise intrusive surveillance. If you are asked by another agency to co-operate with intrusive surveillance, you should seek advice from the Director Law and Governance immediately. Where other authorities say that they are authorised to undertake intrusive surveillance but need our co-operation, we need to check that their authorisation is in order.

7. What is a covert human intelligence source?

7.1 A covert human intelligence source (CHIS) is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or council officer to strike up a relationship with someone as part of an investigation to obtain information "under cover".

7.2 The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):

a. the identity of the source.
b. the identity, where known, used by the source.
c. any relevant investigating authority other than the authority maintaining the records.
d. the means by which the source is referred to within each relevant investigating authority.
e. any other significant information connected with the security and welfare of the source.
f. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source.
g. the date when, and the circumstances in which, the source was recruited.
h. the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c).

i. the periods during which those persons have discharged those responsibilities.
j. the tasks given to the source and the demands made of him in relation to his activities as a source.
k. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority.
l. the information obtained by each relevant investigating authority by the conduct or use of the source.
m. any dissemination by that authority of information obtained in that way; and
n. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

7.3 Someone who volunteers information to the council, either as a complainant (for instance, about anti-social behaviour or a breach of planning regulations) or out of civic duty, is unlikely to be a covert human intelligence source. If someone is keeping a record, say, of neighbour nuisance, this will not amount, by itself, to use of a covert human intelligence source. However, if we are relying on, for example, a neighbour to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source.

7.4 The use by the council of covert human intelligence sources is expected to be extremely rare and, for that reason, this operational guidance does not deal with the issues to which they give rise. If you are contemplating use of a covert human intelligence source, please take advice from the Director Law and Governance before implementing any plan.

8. Authorising Directed Surveillance/CHIS: The Rules

8.1 It is crucial that all directed surveillance is properly authorised. The advantages of getting it right is that as the authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation then it shall be "lawful for all purposes" and therefore not subject to any civil or criminal liability. As long as all procedures are correctly followed then the likelihood of any evidence obtained being excluded as being unlawful is reduced. The council is subject to audit and inspection by the Office of the Surveillance Commissioner and it is important that we can demonstrate compliance with RIPA and with this operational guidance. Since 2012 it has been necessary to obtain judicial approval from a magistrate. The below details this process.

Who can authorise directed surveillance/CHIS?

8.2 Authorisations may only be given by the officers identified in Appendix A to this operational guidance referred to as "authorising officers" and must be in writing. Where practical, the authorising officer should not be directly involved in the case giving rise to the request for authorisation. An authorising officer may authorise a request made by staff who report to them if they are not directly involved in the case. Where it is not practical for authorisation to be given by an officer who is not directly involved, this should be noted with reasons on the authorisation form.

On what grounds can directed surveillance/CHIS be authorised?

8.3 Directed Surveillance can only be authorised if it is necessary on certain statutory grounds. The only ground the council can use is where surveillance is necessary to:

- **prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months imprisonment or;**
- **are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.**

Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least six months' imprisonment'

8.4 Local Authorities are only permitted to authorise a CHIS where the authorising officer believes that the authorisation of a CHIS is necessary under s29(3)(b) namely that it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

8.5 Please note that surveillance/CHIS has to be **necessary** for this purpose. If you can reasonably obtain the information by other means then the directed surveillance was not necessary and therefore not justifiable in the circumstances. "Necessity" is something that needs to be looked at on a case by case basis.

Once necessity is established then is the proposed surveillance proportionate?

8.6 Authorisation should not be sought, and authority should not be given unless the authorising officer is satisfied that the directed surveillance is proportionate to what is being sought to be achieved. This means you should make sure that the end being sought justifies any interference with privacy. If the benefit to be obtained from surveillance is marginal, or if the problem you are seeking to tackle is not very serious, you should think very carefully about whether the use of surveillance is appropriate and therefore proportionate.

8.7 The test should be "in the light of the seriousness of the breach of law is what is proposed excessive and is there a less invasive way to find the information".

8.8 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone make intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of surveillance techniques would be disproportionate.

8.9 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 offence;
- 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 necessary result;
- Evidencing, as far as reasonable practical, what other methods had been considered and why they were not implemented.

Is the proposed surveillance discriminatory?

8.10 The council is under a legal obligation to avoid either direct or indirect discrimination in carrying out its functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the Human Rights Act. You should be sensitive to this issue and ensure that you apply similar standards to seeking or authorising surveillance regardless of ethnic origin, sex or sexual orientation, disability, age etc. You should be alert to any stereotypical assumptions about people from different backgrounds.

Might the surveillance involve "collateral intrusion"?

8.11 In other words, might the surveillance intrude upon the privacy of people other than those who are the subject of the investigation? You should be sensitive to the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified when balanced with the benefits of undertaking the surveillance.

Might the surveillance involve acquiring access to any confidential or religious material?

8.12 If so, then the surveillance will require a particularly strong justification and arrangements need to be put in place to ensure that the information obtained is kept secure and only used for proper purposes. Confidential material might include legal or financial records, or medical records. Where there is a possibility that access to confidential or religious material might be obtained, the authorisation of the Chief Executive (who will consult with the Director Law and Governance) must be sought.

9. Authorising Directed Surveillance: The Procedure

9.1 Applying for authorisation- at the outset a Unique Reference Number (URN) must be obtained from the EA to the Director, Law and Governance. It is very important that this is done even if the application does not proceed or is not authorised as both these incidents need to be recorded for audit purposes.

9.2 Applications for authorisation must be made on the correct form (with a URN), except in case of extreme urgency, in which case written authorisation should be

sought at the earliest opportunity. The form to seek authorisation can be accessed at Appendix B to this operational guidance.

9.3 A written application for authorisation for directed surveillance should describe in detail any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case for the purpose of preventing or detecting crime;
- the grounds upon which it is sought;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve eg could the information be achieved by other means?
- the nature of the surveillance eg where will officers be located, will they use a vehicle, what equipment will be used?
- the identities, where known, of those to be the subject of the surveillance; or if for a specific operation that is for the purpose of identifying the persons causing the problem then that should be stated;
- an explanation of the information which you want 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 level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

9.4 Once the application has been authorised by an authorising officer, an application should be made to the Magistrates Court to hear the matter for judicial approval in consultation with legal services.

10. Duration of authorisations

10.1 Judicial approval granted by a magistrate will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect in respect of Directed Surveillance and **12 months for a CHIS** (1 month if the CHIS is 18).

10.2 Even though authorisations cease to have effect after three months/12 months, you should not simply leave them to expire. When the surveillance ceases to be necessary, you should always follow the cancellation procedure. See section 13. Where surveillance has ceased, we must be able to match each authorisation with a timed and dated cancellation.

11. Reviews

11.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue.

11.2 The maximum period between authorisation and review, and between reviews, should be four weeks. The more significant the infringement of privacy, the more frequent should be the reviews.

11.3 The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion. Reviews are also essential for future reference so that we can see as an organisation how we are doing and learn from the successes and failures of authorisations.

11.4 In each case authorising officers within the council should determine how often a review should take place. This should be as frequently as is considered necessary and practicable by the authorising officer.

11.5 The form to record a review of an authorisation is accessible at Appendix B to this operational guidance.

11.6 A review may result in a new and different authorisation being necessary (e.g. where the subject of the surveillance or the location of the surveillance changes).

12. Renewals

12.1 A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by the Magistrate.

12.2 All applications for the renewal of an authorisation for directed surveillance should be made on the form accessible at Appendix B to this operational guidance and should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

- any significant changes to the information given in the original application for authorisation;

- the reasons why it is necessary and proportionate to continue with the directed surveillance;

- the content and value to the investigation or operation of the information so far obtained by the surveillance;

- the date and time of each renewal;

- the results of regular reviews of the investigation or operation.

12.3 The renewal should be kept and recorded as part of the central record of authorisations.

12.4 It is unlikely that authorisations will be renewed very often and officers will need to be quite clear what extra information they expect to collect after an initial 3 months of covert surveillance (12 months using a CHIS).

13. Cancellations

13.1 The authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was issued.

13.2 Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer.

13.3 If in doubt about who may cancel an authorisation, please consult Director Law and Governance.

13.4 Cancellations are to be effected by completion of the form accessible in Appendix B to this operational guidance.

N.B. Please note the warning that there must be a completed, timed and dated cancellation for each authorisation once surveillance has been completed. An authorisation should not be allowed to expire.

14. Ceasing of surveillance activity

14.1 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s).

14.2 The date and time when such an instruction was given should be included in the central record of authorisations.

14.3 There is no need for any application to the Magistrates Court in respect of cancelling any authorisation or ceasing surveillance activity.

15. Record Keeping and Central Record of Authorisations

15.1 A centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request.

15.2 The Principal Children's Services Lawyer is responsible for the management of the Central Register.

15.3 These records should be retained for a period of at least three years within a centrally retrievable file managed by the Principal Children's Services Lawyer from the ending of the authorisation and should contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- for local authorities, details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- the dates of any reviews;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal (Magistrates details), including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled.

15.4 In all cases, the relevant authority should maintain the following documentation for at least three years and will be managed by the Principal Children's Services Lawyer:

15.5 The following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a 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 to cease surveillance was given;
- the date and time when any other instruction was given by the authorising officer;
- for local authorities a copy of the order approving or otherwise the
- grant or renewal of an authorisation from a Justice of the Peace (Magistrate).

15.6 In addition, copies of the following must be sent to the Director Law and Governance immediately upon completion:

- all completed forms authorising directed surveillance/CHIS;
- all completed review forms
- all completed forms authorising renewal of directed surveillance;
- all completed forms cancelling directed surveillance.
- Any other directions given by the authorising officer.

These will be kept and reviewed by the Principal Children's Services Lawyer at least every twelve months.

15.7 Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially where it is necessary to act urgently.

15.8 Where an authorising officer authorises such an investigation or operation the central record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

16. Authorising Use of Covert Human Intelligence Sources

16.1 Similar principles and procedures apply to authorising the use of covert human intelligence sources which will only be used in exceptional circumstances.

16.2 If it becomes apparent that their use is more than very exceptional, detailed guidance will be published and circulated.

16.3 For the present, officers' attention is drawn to the explanation of the nature of a covert human intelligence source in Paragraph 6.

16.4 If you think you might be using, or might use, a covert human intelligence source, please contact the Director Law and Governance, who will advise on the principles to be applied, the authorisation procedure, record keeping etc.

16.5 For the avoidance of doubt, the Council will comply, so far as applicable, with the Code of Practice issued by the Home Office.

17. Internet and social networking sites

17.1 Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether a RIPA authorisation should be obtained.

17.2 Where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, a RIPA authorisation should be considered. When conducting an investigation which involves the use of the internet factors to consider are:

- If an investigating officer views a Facebook profile with whom they are not 'friends' and the profile is not protected by any privacy settings the information can be treated as being in the public domain. Any initial viewing/visiting of this profile will be overt and authorisation under RIPA will not be required.

- If the officer frequently or regularly views the same individual's profile this is considered targeted surveillance and a RIPA authorisation is required.

- If an investigating officer enters into a 'conversation' with a profile, and the officer informs them that he is contacting them in his role as an employee of MKC, then this contact will be overt and no authorisation will be required.

- Officers must not create a false identity in order to "befriend" individuals on social networks without an authorisation under RIPA;

- Officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation;

- Repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once a RIPA authorisation has been granted and approved by a Magistrate; and

- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

17.3 Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites without disclosing his or her identity, a Covert Human Intelligence Source authorisation should be considered and in place.

17.4 Passing an access control so as to look deeper into the site, for example by making a 'friend request', requires at least directed surveillance authorisation. If the investigator is to go further and pursue enquiries within the site, thereby establishing a relationship with the site host in the guise of a member of the public, this requires CHIS authorisation.

17.5 Further guidance, with illustrative examples, is provided in the Home Office's Revised Code of Practice on Covert Surveillance and Property Interference in the section on Online Covert Activity, pages 18-21 at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

17.6 Officers should not use their own accounts for work purposes and certainly not for any surveillance.

18. Training

18.1 All relevant Heads of Service/ Directors should ensure that those of their staff who are likely to use these procedures have been properly trained to do so. It is particularly important that new recruits to a service have their training needs assessed and that any identified needs are met promptly.

18.2 Officers engaged in investigatory or enforcement areas where RIPA considerations may apply they must ensure they have maintained their levels of knowledge and if unsure seek advice from legal services.

19. Monitoring

19.1 The Director of Law and Governance is responsible for monitoring the implementation of all changes and recommendations arising from any change in legislation and following the inspection by the Investigatory Powers Commissioner's Office.

19.2 The Principal Lawyer for Children's Social Care is responsible for ensuring an annual review of all policies and ensure deletion of any documents is in line with the agreed retention period and the Data Protection Act.

20. Errors

20.1 An error must be reported if it is a "relevant error". Under section 231(9) of the 2016 Act, a relevant error for the purpose of activity covered by this code is any error

by a public authority in complying with any requirements that are 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 the 2000 Act or the property interference provisions of the 1994 and 1997 Acts.

20.2 Examples of relevant errors occurring would include circumstances where:

• Surveillance or property interference activity has taken place without lawful authorisation.

• There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Code of Practice.

20.3 All relevant errors made by public authorities must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error. The error must be reported to the Director of Law and Governance immediately. The Director of Law Governance shall then take the following steps:

- Provide a detailed report to the Investigatory Powers Commissioner as soon as is reasonably practicable and within ten working days. If this is not possible reasons must be provided.
- The report should include information on the cause of the error; the amount of surveillance or property interference conducted 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

20.4 In relation to serious errors, Section 231 of the 2016 Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error.

20.5 The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

20.6 Before making his or her decision, the Commissioner must ask the public authority which has made the error to make submissions on the matters concerned. Public authorities must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

Appendix A: Approved Authorising Officers for the Purposes of the Regulation of Investigatory Powers Act 2000

- Chief Executive – Michael Bracey
- Director Law and Governance and Monitoring Officer – Sharon Bridglalsingh
- Head of Legal Services and Deputy Monitoring Officer – Catherine Stephens
- Head of Regulatory Services – Neil Allen
- Chief Internal Auditor – Jacinta Fru

APPENDIX B: RIPA FORMS

All forms can be downloaded from:
RIPA forms - GOV.UK (www.gov.uk)
It is your responsibility to ensure that you are using the current version of the RIPA forms.

The form to be used for applications for Magistrate approval, in both the Directed Surveillance and CHIS sections is at: http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

Directed surveillance

1. Application for Directed Surveillance Authorisation
2. Review of Directed Surveillance Authorisation
3. Cancellation of Directed Surveillance Authorisation
4. Renewal of Directed Surveillance Authorisation
5. Magistrate approval of authorisation/renewal

Covert Human Intelligence Sources

1. Application for use of CHIS
2. Review of CHIS Authorisation
3. Cancellation of CHIS Authorisation
4. Renewal of CHIS Authorisation
5. Magistrate approval of authorisation/renewal

Please also see:

Home Office Guidance to Local Authorities, at: Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA):Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance (publishing.service.gov.uk)

In particular, the application process to the Magistrates is explained from page 10 onwards.