OXFORDSHIRE COUNTY COUNCIL

# Cabinet
# Tuesday, 23 January 2024

# ADDENDA 3

**10. Report on the Authority's Policy for compliance with the regulation of the Investigatory Powers Act 2000 , the use of activities within the scope of this act and the recent inspection by the Investigatory Powers Commisioner's Office** (Pages 1 - 14)

RIPA Policy 2023 Annex attached

This page is intentionally left blank

**OXFORDSHIRE COUNTY COUNCIL**

**POLICY ON COMPLIANCE WITH THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)**

# 1. Introduction

1.1 **Where RIPA applies**

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert surveillance activities by Local Authorities. The need for special authorisation arrangements must be considered whenever the Local Authority considers commencing a covert surveillance operation or obtaining information by the use of informants or officers acting in an undercover capacity. Informants are termed covert human intelligence source or CHIS.

1.2 **Social media, confidential information and juveniles**

The authorisation requirements under RIPA may also apply to the monitoring of use of social media. Detailed discussion on this appears in paragraph 6 below. Special procedures also apply where juveniles are involved or where confidential information is sought. Guidance appears in sections 8 and 9 respectively.

**1.3 Surveillance that falls outside RIPA**

Local Authorities operate covert activities in a number of key areas.

Activities can include covert surveillance in relation to Internal Audit and Human Resources where fraud, deception or gross misconduct by staff might be suspected.

RIPA only applies where the Local Authority is investigating crime and exercising one of its core activities or one its specific public functions. It does not apply in the exercise of general and civil matters such as monitoring of human resource policies. Article 8 of the Human Rights Act which protects a person's right to privacy is relevant. A guide to covert activities that fall outside RIPA but under Article 8 appears at section 7 below.

1.4 **Relevant guidance**

The following material is relevant and should guide your actions:

a) The Regulation of Investigatory Powers Act 2000 (as amended);

b) Statutory instrument 2010 No. 521 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010) This sets out the rank of officers who can give a RIPA authority;

c) The Codes of Practice. If in doubt have a look at the Codes listed in 1.4 (c) (i-iii). They offer detailed and practical advice. They give a lot of case studies which might match the scenario you are looking at. You can find them on-line if you simply type the title into google. They are as follows:

i. Covert Surveillance and Property Interference - August 2018;
ii. Covert Human Intelligent Sources – Revised Code of Practice December 2022;

iii. Communications Data – November 2018 (Under Investigatory Powers Act 2016).

To find all the codes follow this link –
https://www.gov.uk/government/collections/ripa-codes

1.5 **Authorisation of covert surveillance or a CHIS**
You will need authorisation from a senior officer where RIPA applies. There are only a small number of Authorising Officers who can give this permission as set out in Appendix 1. Before authorisation it will normally be necessary to consult with the relevant Deputy Director/Assistant Director/Head of Service. You should discuss the matter with your Line Manager before seeking authorisation.

**1.7 Application of policy**
This Policy applies to all services in Oxfordshire County Council. The Trading Standards Service has their own specific internal Service procedures for dealing with authorisations. Copies of all authorisations including those for Trading Standards will be forwarded to the Head of Trading Standards for retention in a central register.

**1.8 Safeguarding**
It is imperative that the safety and welfare of young people is prioritised in any covert surveillance involving or relating to juveniles. This is outlined further in section 8.

## 2. Definitions

**Surveillance** – includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

**Covert Surveillance** – this is carried out to ensure the person who is the subject of the surveillance is unaware that it is or may be taking place.

Local authorities are able to use the following forms of surveillance which require a RIPA authority:

a) **Directed Surveillance** – is covert but not intrusive, is undertaken for the purposes of a specific investigation which is likely to result in the obtaining of private information about a person (targeted or otherwise);

b) **Covert Human Intelligence Source** (CHIS) – this is an undercover operation whereby an informant or undercover officer establishes or maintains some sort of relationship with the person in order to obtain private information;

c) **Intrusive Surveillance -** means covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle and that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Local Authorities are not lawfully able to carry out intrusive surveillance.



## 3. RIPA Requirements

3.1 **General**

Directed surveillance or the use of a CHIS can only be authorised under RIPA if it involves a criminal offence punishable by a custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol, tobacco or nicotine inhaling products. Less serious criminal offences cannot be subject to directed surveillance under RIPA.

3.2 In either case surveillance under RIPA is only permitted for the purpose of prevention or detection of crime or preventing disorder.

3.3 The surveillance must also be necessary and proportionate. These terms are discussed in paragraphs 4 and 5 below. It should also be subject to review.

3.4 **Prior authorisation**

All directed surveillance and activity by a CHIS require prior authorisation by the appropriate Local Authority Officer (as set out in Appendix 1 of this policy) before any surveillance activity takes place. The only exception to this is where covert surveillance is undertaken by way of an immediate response to events that means it was not foreseeable and not practical to obtain prior authorisation.

3.5 **Who can grant RIPA authority**

Only officers listed in Appendix 1 of this RIPA Policy may authorise surveillance. Special rules apply when authorising the use of a juvenile as a CHIS and this requires a higher level of authorisation as set out in this Policy.

3.6 **Necessary and proportionate**

The surveillance must also be necessary and proportionate. These terms are discussed in paragraphs 4 and 5 below. It should also be subject to review.

3.7 **Judicial approval**

Judicial approval is also required before any internal authorisation of surveillance under RIPA takes effect. Once internal authorisation has been granted a specific application to the Magistrates Court will be required.

3.8 **Criminal Conduct**

Special rules exist where the CHIS activities include criminal conduct under the Covert Human Intelligence Sources (Criminal Conduct) Act 2021. Local Authorities do not have the power to grant criminal conduct authorisations. Be very careful over possible criminal conduct and refer to the Monitoring Officer if in doubt.

3.9 **Intrusive Surveillance**

Local Authorities are not permitted to carry out Intrusive Surveillance. Local Authorities may not use hidden officers or concealed surveillance devices within a person's home or vehicle in order to directly observe that person.

3.10 A flow chart showing the authorisation procedures for covert surveillance and the relevant considerations at each stage is included in Appendix 2 of this policy.

3.11 **Details of procedure to follow in application**

Further details of the procedure to follow including the forms to use are set out in paragraph 12 below.

3.12 **Duration of authorisation**

The duration of authorisation is always three months for directed surveillance and 12 months for a CHIS. However, authorisation should be reviewed periodically and cancelled once the surveillance has achieved its purpose or is no longer required.

3.13 **Failure to obtain a RIPA authority and judicial approval**

If you carry out directed or CHIS surveillance in the absence of a RIPA authority you could be accused of breaching a person's right to privacy under Article 8 of the European Convention on Human Rights. If you wish to use the evidence from an investigation in court the court may exclude the evidence. The Investigatory Powers Tribunal is able to investigate complaints from anyone who feels aggrieved by a public authority's exercise of its powers under RIPA. They are also able to give directions and make awards of damages. You could also face a claim under the Human Rights Act.

## 4. Grounds of Necessity and collateral intrusion

4.1 The authorisation by itself does not ensure lawfulness, as it is necessary also to demonstrate that the interference was justified as both necessary and proportionate. The statutory grounds of necessity must apply for the purposes of preventing or detecting crime or of preventing disorder.

## 5. Proportionality

5.1 **Do the ends justify the means?**

Once a ground for necessity is demonstrated, the person granting the authorisation must also believe that the directed surveillance or use of CHIS is proportionate to what is aimed to be achieved by the conduct and use of that source or surveillance. This involves balancing the intrusive nature of the investigation or operation and the impact on the target or others who might be affected by it against the need for the information to be used in operational terms. Do the ends justify the means? Other less intrusive options should be considered and evaluated. All RIPA investigations or operations are intrusive and should be carefully managed to meet the objective in question and must not be used in an arbitrary or unfair way.

5.2 The following guidance in the Covert Surveillance and Property Interference Code of Practice 2018 should be noted:

'*4.6 The authorisation or warrant 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 render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.*

*4.7 The following elements of proportionality should therefore be considered:*

*• balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;*

*• explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*

*• considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;*

*• evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented or have been implemented unsuccessfully*."

5.3 **Collateral intrusion**

Before authorising applications for directed surveillance, the Authorising Officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance (Collateral Intrusion). Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. Measures should be taken wherever practicable to avoid unnecessary intrusion into the lives of those not directly connected with the operation. All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this to enable the Authorising Officer fully to consider the proportionality of the proposed actions.

## 6. Social Media

6.1 Social media is becoming an increasingly important source of information. Reference should be made to the covert surveillance and property interference Code of Practice 2018 at page 18, 3.10.

6.2 Although most social media sites allow public access, the Code of Practice suggests that prolonged and systematic surveillance of a particular individual on a site would amount to directed surveillance and a RIPA authority should be obtained. The code sets out the checklist of questions in 6.2.1 and where the answer to some or all of them is 'yes' then it's likely that a RIPA authority for directed surveillance is required.

6.2.1 Checklist of questions:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

6.3 Officers must not create a false identity in order to 'befriend' individuals on social networks other than in accordance with the RIPA Codes and with appropriate authorisation.

6.4 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.

## 7 Applications for civil directed surveillance that fall outside RIPA

7.1 RIPA authorities are only available where the Local Authority is involved in preventing or detecting crime or preventing disorder. They are not therefore available where you wish to use covert directed surveillance in the pursuit of civil matters such as employment issues or civil claims. You can however still pursue covert surveillance because the I*nvestigatory Powers Tribunal case of C v the Police (2006)* states that RIPA authorities are only required where a Local Authority is pursuing their core activities rather than general activities that might affect all bodies. A Local Authority as a public body is however subject to Article 8 of the Human Rights Act, the right to privacy which states:-

***'Article 8 – Right to respect for private and family life***

*'Everyone has the right to respect for his private and family life, his home and his correspondence.*

*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.'*

7.2 Where it is wished to pursue covert directed surveillance that falls outside RIPA an internal authorisation process must still be followed. You should also consider whether the surveillance is necessary and proportionate as set out in paragraphs 4 and 5 above. You should also consider the application of Article 8 and record whether the interference is a justified one as set out in Article 8. The Authorising Officer should record their decision in writing, and it should be retained in accordance with the provisions for document retention in this policy. The Head of Trading Standards should also be informed so that a record can be made in the authority's central register of surveillance authorisations. It should be subject to the same periodic reviews. It is not, however, necessary to obtain judicial approval for authorisations that fall outside RIPA.

## 8. Juveniles

### 8.1 Authorisation of a juvenile as a CHIS

Special care should be taken over the authorisation of a juvenile as a CHIS. You should first speak to the Head of Trading Standards. You should read 4.2 and 4.3 of the CHIS Code of Practice 2018 before doing this. They state inter alia**:**

(a) *On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them.*
(b) *In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.*
(c) *Enhanced authorisation is required. Authorisations for juvenile sources should be granted by the Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service.*
(d) *The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.*
(e) *Public authorities must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g. someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). Any deployment of a juvenile CHIS should be subject to the enhanced risk assessment process set out in the statutory instrument, and the rationale recorded in writing.*

### 8.2 Juveniles and directed surveillance

You are referred to the sections on necessity and proportionality that appear in paragraphs 4 and 5 above. If a juvenile is the subject of directed surveillance or there is a risk of collateral intrusion affecting a juvenile, then special care should be taken. The tests of necessity and proportionality that you apply should be more exacting. It is more difficult to justify intrusion into the privacy of juveniles. A risk assessment is required setting out the risks to the juvenile and how those risks will be managed. The application for surveillance authorisation should consider those risks and show why the directed surveillance is necessary and that the ends justify the means. You should record in any application or authorisation that you have taken into account the fact that juveniles are involved. You should record that you have applied an enhanced test.

## 9. Confidential and Privileged Information including information subject to legal professional privilege.

9.1 Special care should be taken where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source.

9.2 Reference should be made to the guidance which appears at Chapter 9 of the Covert Surveillance and Property Interference Code of Practice (August 2018). Detailed considerations apply and you require enhanced levels of authorisation which differ from the usual level of authorisation. Where an investigation may reveal sensitive and confidential material this requires special authorisation by the Chief Executive or his/her delegated Authorising Officer. The provisions are involved and sensitive and you are advised to take advice before proceeding.

## 10. Information security and retention of RIPA authorisations

10.1 It is essential that all information gathered through covert surveillance activities is stored securely, with access strictly restricted to those who require access, and disposed of securely when no longer required for the purpose for which the surveillance was undertaken. The arrangements for storing and disposing of the material gathered through the surveillance should be set out in the application.

10.2 The Deputy Director/Assistant Director/Head of Service for the service area undertaking surveillance retains responsibility for secure storage and disposal of material gathered through surveillance activities. Care should be taken to limit the number of copies of the material, including when providing access to the material to other parties who require it (e.g. legal advisors) and to ensure all copies are disposed of in accordance with retention policies.

10.3 The originals of all authorisations, reviews, renewals, cancellations, Court approvals and details of the dissemination of the product of surveillance must be promptly submitted by the officer on the case to the Head of Trading Standards who shall be the 'RIPA Coordinator'. The Head of Trading Standards will maintain a central register of all cases of Directed Surveillance and CHIS authorisations. The central register shall be stored securely.

10.4 The retention period for the forms which constitute the central register shall be for 5 years**.** This retention period is considered adequate but not excessive for facilitating independent external inspection.

10.5 In all cases, the RIPA coordinator must maintain the following documentation:

a) the application and the authorisation, together with any supplementary documentation and notification of the approval given by the Authorising Officer;
b) the court approval;
c) a record of the period over which the surveillance has taken place;
d) the frequency of reviews prescribed by the Authorising Officer;
e) a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
f) the date and time when any instruction was given by the Authorising Officer;
g) details of persons in possession of the product of surveillance, i.e. the dissemination record.

## 11. **Dissemination, copying and retention of material obtained through authorised surveillance**

11.1 Dissemination, copying and retention of material obtained through the authorised surveillance must be limited to the minimum necessary for authorised purposes. Authorised purposes for the dissemination, copying and retention of material obtained through surveillance are if that processing of the material:

a) is, or is likely to become, necessary for any of the statutory purposes set out in legislation in relation to covert surveillance including RIPA;
b) is necessary for facilitating the carrying out of the functions of public authorities in legislation in relation to covert surveillance including RIPA;
c) is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
d) is necessary for the purposes of legal proceedings; or

e) is necessary for the performance of the functions of any person by or under any enactment.

11.2 All data obtained under RIPA should be clearly labelled and stored with a known retention policy.

11.3 Material obtained from surveillance should only be retained so long as it is necessary for the authorised purpose it should be subject to periodic review. All persons to whom the information is disseminated should be made aware of this principle and review should be carried out by the RIPA coordinator to make sure that they have not retained the information longer than is necessary. All emails or other forms of communication disseminated material should contain a statement recording that the information should not be retained longer than is necessary.

11.4 Particular care should be taken in the storage and destruction of confidential or privileged material such as journalistic material, material subject to legal professional privilege or confidential personal information.

11.5 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Local Authority must ensure that the material is clearly identified and kept securely.

11.6 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

11.7 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

## 12. Implementation of all procedures

12.1 All directed surveillance and CHIS authorisation should be made by the Authorising Officers listed in Appendix 1.

12.2 All applications for authorisation and authorisations must be made in accordance with the procedure and on the appropriate forms: (download forms from the following link: http://intranet.oxfordshire.gov.uk/cms/content/ripa-policy-surveillance)

RIPA Form 1 – Authorisation Directed Surveillance
RIPA Form 2 – Review of a Directed Surveillance Authorisation RIPA Form 3 – Renewal of a Directed Surveillance Authorisation RIPA Form 4 – Cancellation of a Directed Surveillance Authorisation
RIPA Form 5 – Authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)
RIPA Form 6 – Review of a Covert Human Intelligence Source (CHIS) Authorisation
RIPA Form 7 – Renewal of a Covert Human Intelligence Source (CHIS) Authorisation
RIPA Form 8 – Cancellation of an Authorisation for the use or conduct of a Covert Human Intelligence Source (CHIS)
RIPA Form 10 –Judicial Approval Application

12.3 The Senior Responsible Officer will monitor the central register periodically and produce an annual report to the Strategic Leadership Team (SLT) and the Audit & Governance Committee. Renewal of authorisation will be for 3 months. Cancellation of authorisation should be requested as soon as possible i.e. as soon as the surveillance is no longer considered necessary.

12.4 After internal authorisation of an application, judicial approval is required before the operation can commence. The applicant should liaise with the Local Authority's Legal Service for advice and assistance in making this application for judicial approval (other than Trading Standards applications which are managed within the service). Judicial approval is required for the renewal of authorisation, but it is not required for any internal review or cancellation.

12.5 The Authorising Officers may authorise a person to act in their absence. The substitute will be a senior manager and who will have overall management responsibility for the operation/investigation. A list of all current named Authorising Officers and named substitutes will be included in the central register and appended to this Policy (Appendix 1). The Director of Law and Governance will approve all proposed Authorising Officers for inclusion in a central register. The annual report to SLT and the Audit & Governance Committee will also include a review of the appropriate designated Authorising Officers.

12.6 All managers have responsibility for ensuring that they have sufficient understanding to recognize when an investigation or operation falls within the requirements of RIPA. Authorising Officers will keep up to date with developments in the law and best practice relating to RIPA.

12. 7 Authorising Officers must ensure full compliance with the RIPA Authorisation Procedure set out in the appropriate forms in paragraph 12.2 above.

12.8 Authorising Officers and Deputy Directors/Assistant Directors/Heads of Service will co-operate fully with any inspection arranged by the Investigatory Powers Commissioner's Office.

12.9 **RIPA Coordinator (Head of Trading Standards)**

The role of the RIPA Coordinator is to have day-to-day oversight of all RIPA authorisations and maintain a central register of all authorisations, review dates, cancellations and renewals.

All forms should be passed through the RIPA Coordinator to ensure that there is a complete record of all authorisations. Contents of the forms will be monitored to ensure they are correctly filled in and the coordinator will supply quarterly statistics to the Senior Responsible Officer (Director of Law and Governance and Monitoring Officer).

The Coordinator will also monitor training requirements and organise training for new staff as appropriate and ensure continued awareness of RIPA throughout the Council via staff information on the Council's Intranet.

## 13. Communications Data

Local authorities can obtain a very limited amount of communications data. This falls under the Investigatory Powers Act 2016 and not RIPA. Separate procedures and law apply. It is unlikely that you would ever seek communications data. If you do need to seek access to communications you should contact the Head of Trading Standards for guidance.

## 14. Briefings

The Director of Law and Governance will provide updates on the RIPA legislation and best practice but Assistant/Deputy Directors/Heads of Service and other managers must be able to recognise potential RIPA situations.

## 15. Conclusion

The benefit of having a clear and regulated system of authorising all covert activities is self-evident. Surveillance by its very nature is intrusive and therefore should be subject to appropriate scrutiny at the highest level and the authorisation procedure requires that the reasons for the decision are specifically and clearly set out and the basis for the decision is readily accessible and understood.
Completion of appropriate authorisations also means that in reaching a decision alternative options will also have been fully explored. Proper compliance with the procedure and properly recorded authorisations is the best defense should any of our investigations be challenged.

## 16. Review of Authorisations and Policy

16.1 The Council's "Audit and Governance Committee" will review:

a) a summary of all authorised RIPA applications on a regular basis; and
b) an annual report from the Director of Law and Governance on the operation of the Policy; and
c) the policy annually to ensure it remains compliant with current legislation, relevant codes of practice and continue to meet the responsibilities of the Council.

Senior Responsible Officer: Director of Law and Governance and Monitoring Officer

RIPA Coordinator: Head of Trading Standards

Date: January 2024
Next Review Date: January 2025

## Appendix 1
## Authorising Officers and Named Substitutes

Senior Responsible Officer – Anita Bradley, Director of Law and Governance and Monitoring Officer
(Named substitute - Paul Grant, Head of Legal)

Authorising Officer – Jody Kerman, Head of Trading Standards

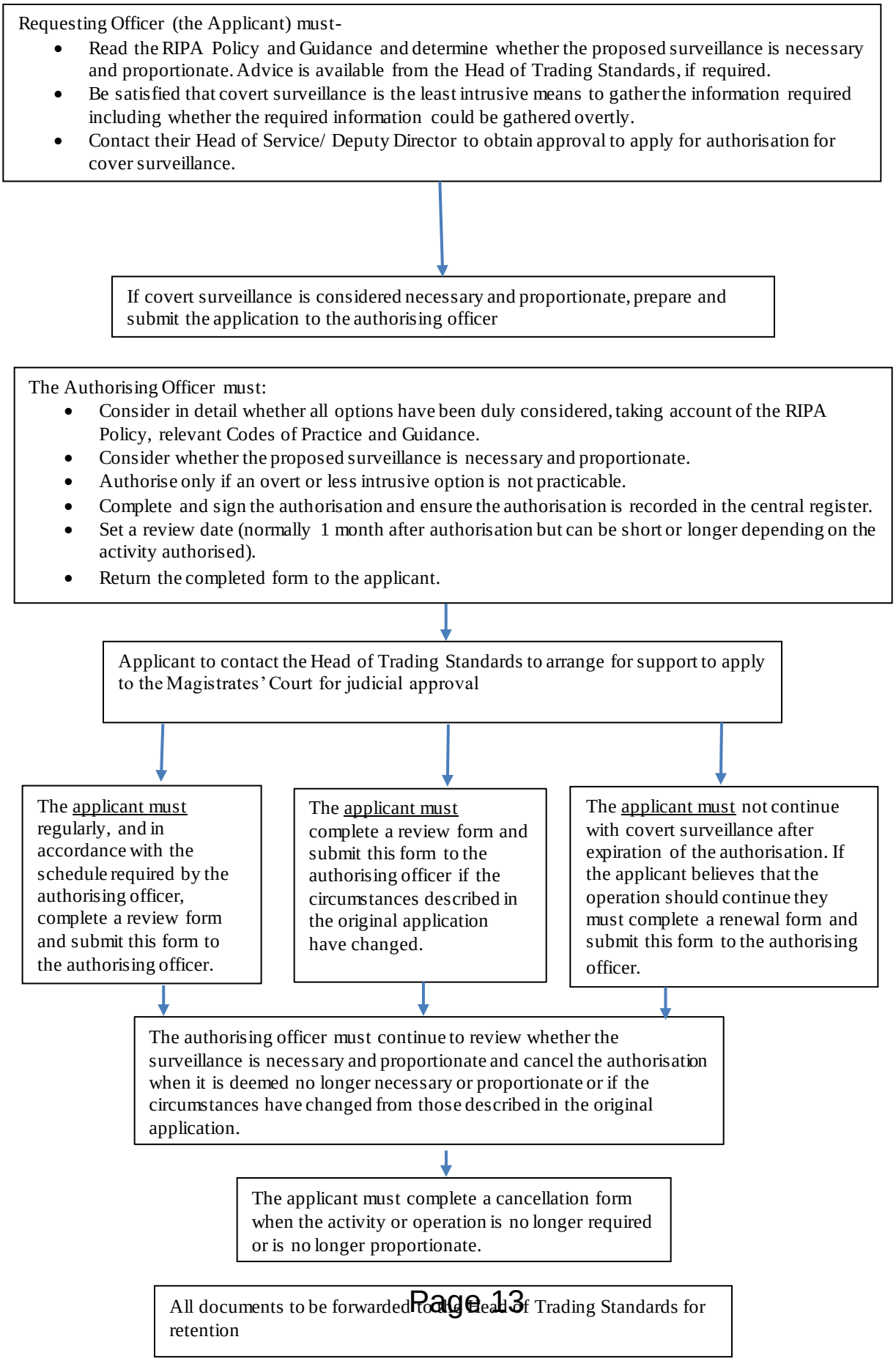
Authorising Officer and Named Substitute – Lorna Baxter, Executive Director of Resources and S151 Officer

Confidential Material Special Authorisation – Martin Reeves, Chief Executive**

**Named Substitute – Lorna Baxter, Executive Director of Resources and S151 Officer

## Appendix 2

## Flow Chart of Authorisation Procedures and Considerations for Covert Surveillance



This page is intentionally left blank