APPENDIX 9

REGULATION OF INVESTIGATORY POWERS ACT 2000

CORPORATE POLICY AND PROCEDURE ON THE USE OF COVERT SURVEILLANCE

Title	Regulation of Investigatory Powers Act 2000
Owner	Director of Resources
Version	2
Issue date	
Approved by	Council
Next revision due	February 2022

Contents

1

INTRODUCTION

1.1 This document sets out the policy and procedures adopted by Maldon District Council ("the council") in relation to Part II of the Regulation of Investigatory Powers Act 2000 ("RIPA"). The policy should be read in conjunction with the Home Office Codes of Practice on covert surveillance and covert human intelligence sources; acquisition and disclosure of communications data, and any guidance issued by the Investigatory Powers Commissioner's Office (IPCO) (formerly the Office of Surveillance Commissioners – OSC)

1.2 For the purpose of this update, references to the Home Office Codes of Practice relate to the latest versions which were issued in August 2018 in relation to covert surveillance and covert human intelligence sources; and 2016 in relation to the acquisition and disclosure of communications data. References to the OSC Procedures and Guidance document relate to the latest version which was issued in July 2016.

1.3 The following terms are used throughout this Policy:

RIPA	Regulation of Investigatory Powers Act 2000
CHIS	Covert Human Intelligence Source
SPoC	Single Point of Contact

SRO	Senior Responsible Officer
IPCO	Investigatory Powers Commissioner's Office
NAFN	National Anti-Fraud Network
CSP	Communications Service Provider

1.4 It should be noted that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless necessary.

1.5 Further information on RIPA forms can be found on the intranet with search word "Ripa"

2 PURPOSE AND OBJECTIVES

2.1 Directed surveillance or acquisition of communications data by or on behalf of the council must be carried out in accordance with this policy. Any such activity must be authorised by one of the Authorising Officers identified in Appendix A. All authorisations must then be approved by a Magistrate before any covert activity takes place. Staff directly employed by the council and any external agencies working for the council are subject to RIPA whilst they are working in a relevant investigatory capacity.

2.2 The purpose of the policy is to ensure the council is acting lawfully while undertaking its various enforcement functions, ensuring directed surveillance, or acquisition of communication data is both necessary and proportionate, and takes into account the rights of individuals under Article 8 of the Human Rights Act.

2.3 Surveillance, for the purpose of the Act, 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.

3 ROLES AND RESPONSIBILITIES

3.1 Senior Responsible Officer (SRO):

3.1.1 The role of SRO will be undertaken by the council's Director of Resources

3.1.2 In accordance with good practice the SRO will be responsible for:

- The integrity of the process in place within the council for the management of covert surveillance;
- Ensuring that all authorising officers are of an appropriate standard;
- Compliance with Part 2 of the Act and with the Home Office Codes of Practice;

- Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable;

- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

- Have overall responsibility for the management and oversight of requests and authorizations under RIPA;

- Retain a copy of the application and authorization together with any supplementary documentation and notification of the approval given by the authorizing officer maintain a central RIPA records file;

- Review and monitor all forms and documents received to ensure compliance with the relevant law and guidance and this policy and procedures document and informing the Authorizing Officer of any concerns;

- Be responsible for organizing a corporate RIPA training programme and ensure corporate awareness of RIPA

3.2 **Authorizing Officers**

3.2.1 The officers named in Appendix A shall be the only officers within the council who can authorize applications under RIPA in accordance with the procedures set out in section 7 of this policy.

3.2.2 Each of the Authorizing Officers can authorize applications, for onward consideration by a Magistrate. Each Authorizing Officer may authorize renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers. Authorizing Officers **may not sub-delegate** their powers in relation to RIPA to other officers.

3.2.3 The officer who authorizes a RIPA application should normally also carry out the review,renewal and cancellation. If the original Authorizing Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorizing Officer.

4 LOCAL AUTHORITY USE OF RIPA

4.1 RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. If such activities are conducted by council

officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.

4.2 RIPA limits local authorities to using three covert techniques, as set out below:

- **Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles
- A **Covert human intelligence source (CHIS)** includes undercover officers, public informants and people who make test purchases (for enforcement purposes)
- Acquisition of **Communications data** is the 'who', 'when' and 'where' of a communication, but not the 'what' (ie the content of what was said or written). RIPA groups communications data into three types:
    - 'traffic data' (which includes information about where the communications are made or received)
    - 'service use information' (such as the type of communication, time sent and its duration); and
    - 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services)

4.3 Under RIPA a local authority can only authorize the acquisition of the less intrusive types of communications data: service use and subscriber information. Under **no circumstances** can local authorities be authorized to obtain traffic data under RIPA.

4.4 Local authorities are **not** permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

4.5 Directed surveillance may only be authorized under RIPA for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco.

4.6 Local authorities cannot authorize 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 6 months' imprisonment. Requests for authorization must still demonstrate how the activity is both proportionate and necessary.

4.7 Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more include more serious criminal damage and dangerous waste dumping

4.8 Directed surveillance will always be a last resort in an investigation, and use of a **CHIS by the council will not as a matter of policy be undertaken and**

therefore the council will not apply for such authorizations.

4.9 In cases of joint working with other agencies, for example the Department for Work and Pensions or the Police, only one authorization from one organisation is required. This should be made by the lead authority for the particular investigation. Council officers should satisfy themselves that authorization has been obtained and be clear exactly what activity has been authorized.

4.10 For access to communication data, a Single Point of Contact (SPoC) is required to undertake the practical facilitation with the communications service provider (CSP) in order to obtain the data requested. The SPoC must have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the local authority and CSP.

4.11 The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications to a Magistrate and an authorizing officer in the council is still required to scrutinise and approve any applications.

4.12 Compliance with the provisions of RIPA, the Home Office Codes of Practice and this policy and procedures should protect the council, its officers and agencies working on its behalf against legal challenge. Section 27 of RIPA states that "conduct…shall be lawful for all purposes if an authorisation…confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation". If correct procedures are not followed, the council could be rendered liable to claims and the use of the information obtained may be disallowed in any subsequent legal proceedings.

5 THE SCOPE OF RIPA AND TYPES OF SURVEILLANCE

5.1 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases investigations carried out by council officers will not be subject to RIPA, as they involve overt rather than covert surveillance (see below). An explanation of terms used is set out below:

5.2 **'Surveillance'** includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications;
- 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.

5.3 Covert Surveillance

- Covert Surveillance is surveillance carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is, or may be taking place.

- RIPA requires the authorisation of two types of covert surveillance (**directed surveillance** and **intrusive surveillance**) plus the use of covert human intelligence sources (CHIS) or acquisition of communications data.

5.4 Directed Surveillance

Directed Surveillance is surveillance which:-

- is covert; and

- is not intrusive surveillance (see definition below - **the council is prohibited by law from carrying out any intrusive surveillance**);

- is not carried out as an immediate response to events where it would not be practicable to obtain authorisation under the Act;

- 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).

5.5 **Private information** in relation to a person includes any information relating to his private and family life, his home and 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. The way a person runs their business may also reveal information about his private life and the private lives of others. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact or associates with.

5.6 Private life considerations are particularly likely to arise if several records are to be analyzed together in order to establish, for example, a pattern of behavior, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gathered may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorization may be considered appropriate

5.7 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a direct surveillance authorization is appropriate.

5.8 Overt Surveillance

5.8.1 Overt Surveillance will include most of the surveillance carried out by the council - there will be nothing secretive, clandestine or hidden about it. For example, signposted CCTV cameras normally amount to overt surveillance . In many cases, officers will be going about council business openly (e.g. a parking attendant patrolling a council car park).

5.8.2 However, care must be taken to ensure that officers are not intentionally acting as members of the public in order to disguise their true intent as this may then be considered as covert and require RIPA authorisation.

5.8.3 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

5.8.4 Overt surveillance does not require any authorisation under RIPA. Neither does **low-level surveillance** consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the Monitoring Officer or the SRO

5.8.5 Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement officers as part of *general* observation does not need to be regulated by RIPA, as long as the *systematic* surveillance of an individual is not involved. However, if binoculars or cameras are used in relation to anything taking place on any residential premises or in any private vehicle the surveillance can be intrusive even if the use is only fleeting. Any such surveillance will be intrusive "if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle". The quality of the image obtained rather than the duration of the observation is what is determinative. **It should be remembered that the council is not permitted to undertake intrusive surveillance.**

5.8.6 Similarly, although signposted CCTV cameras do not normally require authorisation, this will be required if the camera(s) are to be directed for a specific purpose which involves prolonged surveillance on a particular person. (See Section 12 for guidance on the authorisation of directed surveillance undertaken by means of the council's CCTV cameras.)

5.8.7 Use of body worn cameras should be overt. Badges should be worn by officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary – for example, when issuing parking tickets.

5.8.8 Surveillance that is unforeseen and undertaken as **an immediate response** to

events or circumstances such that it is not reasonably practicable to seek authorisation normally falls outside the definition of directed surveillance and therefore authorisation is not required. However, if a **specific investigation** or **operation is subsequently to follow**, authorisation must be obtained in the usual way before it can commence. In no circumstances will any covert surveillance operation be given backdated authorisation after it has commenced.

5.9 **Social Networking Sites (SNS)**

5.9.1 The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (The Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

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

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

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

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.'

5.10 **Intrusive Surveillance**

5.10.1 Intrusive Surveillance occurs when surveillance:

- is covert;
- relates to residential premises and/or private 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.

5.10.2 **Intrusive surveillance cannot be carried out or approved by the council**. Only the police or other law enforcement agencies are permitted to use such powers. Likewise, the council has no statutory powers to interfere with private property.

6 COVERT HUMAN INTELLIGENCE SOURCE

6.1 The use of a covert human intelligence source (CHIS), and his or her conduct, also requires authorisation under RIPA. It is considered unlikely that there will be any circumstances which would require the council to either use a CHIS or operate under cover and so the **Council will not seek authorisations under RIPA for CHIS.** It is however important that employees read this part of the policy so that they do not by accident carry out surveillance that requires authorization.

6.2 A CHIS is defined as someone who establishes or maintains a personal or other relationship for the purpose of

- covertly using the relationship to obtain information or provide access to any

information to another person;
- covertly disclosing information obtained by means of that relationship where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

These provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating "undercover". Great caution should be exercised in these circumstances.

6.3 The provisions of RIPA relating to CHIS do not apply where a situation would not normally require a relationship to be established for the covert purpose of obtaining information. For example:

- where members of the public volunteer information to the council as part of their normal civic duties;
- where the public contact telephone numbers set up by the council to receive information;
- where members of the public are asked to keep diaries of incidents in relation to, for example, planning enforcement, anti-social behaviour or noise nuisance. However, in certain circumstances, RIPA authorisation may be required if the criteria in section 26(2) of the Act are met.

.

7 AUTHORISATION PROCEDURES

7.1 **Any directed surveillance undertaken by or on behalf of the council must be carried out in accordance with RIPA (see section 14 about non ripa) and must not commence until authorisation has been granted and has been approved by a relevant judicial authority**. If such activities are undertaken without authorisation the SRO must be advised immediately. Only those officers employed in the designated "Authorising Officer Posts" set out in Appendix A can authorise an application under RIPA. Once authorised, the application must be presented to a Magistrate for final approval.

7.2 The acquisition of communications data can only be undertaken by a SPoC, although the same authorisation procedures will apply.

7.3 Officers must discuss the need to undertake directed surveillance with their line manager before seeking an authorisation. **All other reasonable and less intrusive options to gain the required information must be considered before an authorisation is applied for and the RIPA application must detail why these options have failed or have been considered not appropriate in the circumstances of the individual investigation.**

7.4 All applications for authorisation must be made on the appropriate form and can be found on the council's intranet by using "Ripa" in the search engine. In the event of any query, officers making or authorising applications should consult the Monitoring Officer or the SRO. Authorisations will not take effect until the relevant judicial authority has made an order approving the grant of the authorisation. The relevant judicial authority in England and Wales is a

Magistrate. **It is vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate**

7.5 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. **There is no requirement for the Magistrate to consider either cancellations or internal reviews.**

7.6 In any case where it is likely that **confidential information** may be acquired by directed surveillance or by the use or conduct of a source, **the Authorised Officer who may grant authorisation is the SRO (Director of Resources) or, in her absence the Monitoring Officer.**

7.7 **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. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality may be involved

7.8 Covert surveillance of all legal consultations should be considered to be intrusive.

7.9 When considering an application, Authorising Officers must:

(a) have regard to the contents of this document, the training provided and any other guidance or advice given by the SRO;

(b) satisfy his/herself that the RIPA authorisation will be:

(i) **in accordance with the law**;
(ii) **necessary** in the circumstances of the particular case; and
(iii) **proportionate** to what it seeks to achieve.

(c) assess whether or not the proposed surveillance is proportionate, considering the following elements:

- The custodial sentence applicable to the offence being investigated;
- 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;
- Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all practical alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

(d) take into account the risk of intrusion into the privacy of persons other than

the specified subject of the surveillance (called 'collateral intrusion'), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible (the degree of likely collateral intrusion will also be relevant to assessing whether the proposed surveillance is proportionate);

(e) consider any issues which may arise in relation to the health and safety of council employees and agents, and ensure that a risk assessment has been undertaken if appropriate.

8 If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that date (see below). Records must be kept in relation to all RIPA applications and authorisations by the Authorising Officer and by sending a copy to the SRO for retention.

9 URGENT AUTHORISATIONS

9.1 It is no longer possible for urgent authorisations to be given orally. However, a Magistrate may consider an authorisation out of hours in **exceptional** circumstances.

10 DURATION OF AUTHORISATIONS

10.1 Authorisations will have effect until the date for expiry specified on the relevant form. They must be granted for the designated period of three months for directed surveillance and one month for the acquisition of communications data. **No further operations should be carried out after the expiry of the relevant authorisation unless it has been renewed.** It will be the responsibility of the officer in charge of an investigation to ensure that any directed surveillance is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect.

10.2 Authorisations should be reviewed at appropriate intervals in order to update the Authorising Officer on progress on the investigation and whether the authorisation is no longer required. Review periods should be set by the Authorising Officer, but should normally take place on a monthly basis unless the Authorising Officer considers that they should take place more or less frequently (if so, the reasons should be recorded). If the surveillance provides access to confidential information or involves collateral intrusion, there will be a particular need to review the authorisation frequently. The results of reviews should be recorded.

10.3 Authorisations must be cancelled as soon as they are no longer necessary. Even if an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled. The responsibility for ensuring that authorisations are cancelled rests primarily with the officer in charge of the investigation, who should submit a request for cancellation on the appropriate form. However, if the Authorising Officer who authorised any directed surveillance (or any Authorising Officer who has taken over their duties) is satisfied that it no longer meets the criteria upon which it was authorised, s/he

must cancel it and record that fact in writing even in the absence of any request for cancellation.

10.4 If it is required, a renewal must be authorised prior to the expiry of the original authorisation. Applications for renewal should be made on the appropriate form shortly before the original authorisation period is due to expire. Officers must take account of factors which may delay the renewal process (eg intervening weekends or the availability of the relevant authorising officer and a Magistrate to consider the application). 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. Renewals of an authorisation may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be cancelled and new authorisation sought. The renewal will begin on the day when the original authorisation would otherwise have expired.

11 MATERIAL OBTAINED DURING INVESTIGATIONS

11.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018 and any other legal requirements, including those of confidentiality, and the council's policies and procedures currently in force relating to document retention. The following paragraphs give guidance on some specific situations, but advice should be sought from the SRO where appropriate.

11.2 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with legal disclosure requirements.

11.3 Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

11.4 Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the council, unless directed by any court order, should only be considered in exceptional circumstances, and in accordance with advice from the SRO.

11.5 Where material obtained is of a confidential nature then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;

- Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;
- Confidential material should be destroyed as soon possible after its use for the specified purpose.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the SRO.

ASSESSMENT AND REVIEW

11.6 Following completion of any investigation/operation involving the use of RIPA, an assessment should be undertaken. This should detail the information obtained and how it was used to take the case forward.

11.7 The SRO will undertake periodic reviews of the assessment forms and may provide these records as part of any inspection by the Office of Surveillance Commissioners.

12 CCTV AND DIRECTED SURVEILLANCE

12.1 The use of CCTV must be accompanied by clear signage in order for any monitoring to be overt. If it is intended to use CCTV for covert monitoring, for example by using either hidden cameras or without any signs warning that CCTV is in operation, then RIPA authorisation is likely to be required.

12.2 **Note 272 of the OSC's 2016 Procedures & Guidance document:**

272. It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

13 RECORDS MANAGEMENT

13.1 Records shall be maintained for a period of at least **three years** from the cancellation of the authorisation. Following which they shall be securely destroyed in accordance with the council's Retention and Disposal Policy.

13.2 A copy of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the SRO within **five working days** of the date of the relevant decision. All documents should be sent in sealed envelopes marked "For Your Eyes Only".

13.3 Applicants and Authorising Officers may keep copies of completed RIPA forms, but care must be taken to ensure any copies are stored securely and disposed of in accordance with the council's retention and disposal policy. It is good practice for officers who will be carrying out surveillance to retain a copy of the authorisation as a reminder of exactly

what has been authorised. Under the Criminal Procedure and Investigations Act, case files are required to hold original documents for court action.

13.4 A 'Surveillance Log Book' should be completed by the investigating officer(s) to record all operational details of authorised covert surveillance. Each service will also maintain a record of the issue and movement of all Surveillance Log Books.

13.5 All RIPA records, whether in original form or copies shall be kept in secure locked storage when not in use.

14 NON-RIPA

14.1 It is important to understand that s 80 RIPA has the effect that if covert surveillance takes place without an authorization then it is not necessarily rendered unlawful. The effect of not having an authorization means that the Council cannot claim the protection of s27 which makes any such surveillance expressly lawful.

14.2 There may be circumstances when the crime threshold is not satisfied to apply for authorization under the legislation. However there may be a need to carry out covert surveillance eg employee surveillance. In such a case the forms for directed surveillance should be completed seeking authority from an Authorised Officer so that the Council is obliged to consider the seriousness of its proposed action and the need for rigour in authorizing a non ripa approved surveillance.

15 TRAINING

15.1 Appropriate corporate training will be arranged by the SRO for all officers likely to make applications or authorise them.

15.2 Such Officers must receive training on a bi- annual basis. This may be by way of a briefing or an e-learning module.

15.3 No officer will be permitted to undertake the role of Applicant or Authorising Officer unless she/he has undergone suitable training approved by the SRO

APPENDIX – ROLES AND RESPONSIBILITIES

AUTHORISING OFFICERS

1.Director of Resources

2.Strategic Services Manager

3. Monitoring
Officer

SENIOR RESPONSIBLE OFFICER

Director of Resources