Appendix A

Regulation of Investigatory Powers Act 2000 (RIPA) Policy

Version Control Sheet:

Title:	RIPA Policy.
Purpose:	To advise staff of the procedures and principles to follow to comply with the RIPA Act.
Author:	Lee Henley – Strategic Lead Information Management
Owner:	Ian Hunt – Assistant Director of Law and Governance & Monitoring Officer
Approved by:	Standards and Audit Committee.
Date:	July 2021
Version Number:	4.0
Status:	Final.
Review Frequency:	As and when changes to legislation take place
Next review date:	As and when changes to legislation take place

Amendment History / Change Record:

Date	Version	Key Changes / Sections Amended	Amended By
July 2021	4.0	• Section 4 (points 5 and 9) - The policy is now clear that the Authorising Officer is responsible and/or accountable for the authorisation of applications and not the Senior Responsible Officer (SRO). The SRO role is a quality assurance role (e.g. to ensure the request meets the crime threshold) • Section 5 - The policy is now clear that the Authorising Officer is responsible and/or accountable for the authorisation of applications and not the Senior Responsible Officer (SRO). • Section 10 – The policy now includes specific information regarding the management and retention of directed surveillance records. This includes setting out the arrangements to ensure	Strategic Lead – Information Management

		that directed surveillance records are held for as long as necessary • Section 15 - The policy is clear that records of visits by staff to any social media sites must be documented by staff at all times. A Social Media Activity Log has been set up for service areas to records such checks. The policy also sets out the arrangements in place to check for compliance regarding social media site monitoring	

Contents:

Appendices:

1. A brief overview of RIPA

(For text in **bold**, see glossary of terms – Appendix 1)

The Regulation of Investigatory Powers Act (RIPA) was introduced by Parliament in 2000. The Act sets out the reasons for which the use of **directed surveillance** (DS) and **covert human intelligence source** (CHIS) may be authorised.

Local Authorities' abilities to use these investigation methods are restricted in nature and may only be used for the prevention and detection of crime or the prevention of disorder. Local Authorities are not able to use **intrusive surveillance.**

Widespread, and often misinformed, reporting led to public criticism of the use of surveillance by some Local Authority enforcement officers and investigators. Concerns were also raised about the trivial nature of some of the 'crimes' being investigated. This led to a review of the legislation and ultimately the introduction of the Protection of Freedoms Act 2012 and the RIPA Directed Surveillance and Covert Human Intelligence Source (CHIS) (Amendment) Order 2012.
In addition to defining the circumstances when these investigation methods may be used, the Act also directs how applications will be made and how, and by whom, they may be approved, reviewed, renewed, cancelled and retained.

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA), and the Data Protection Act (DPA).

Further, a Local Authority may only engage the Act when performing its 'core functions'. For example, a Local Authority may rely on the Act when conducting a criminal investigation as this would be considered a 'core function', whereas the disciplining of an employee would be considered a 'non-core' or 'ordinary' function.

Examples of when local authorities may use RIPA and CHIS are as follows:

- Trading standards – action against loan sharks, rogue traders, consumer scams, deceptive advertising, counterfeit goods, unsafe toys and electrical goods;
- Enforcement of anti-social behavior orders and legislation relating to unlawful child labour;
- Housing/planning – interventions to stop and make remedial action against unregulated and unsafe buildings, breaches of preservation orders, cases of landlord harassment;
- Counter Fraud – investigating allegations of fraud, bribery, corruption and theft committed against the Council; and
- Environment protection – action to stop large-scale waste dumping, the sale of unfit food and illegal 'raves'.

The examples do not replace the key principles of necessity and proportionality or the advice and guidance available from the relevant oversight Commissioners.

There are 3 key codes of practice and guidance available in relation to the RIPA Act and these are shown in the links below:

Covert Surveillance and Property Interference - Code of Practice

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Covert Human Intelligence Sources - Code of Practice

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

Communications Data - Code of Practice

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

2. Directed Surveillance

This policy relates to all staff directly employed by Thurrock Council when conducting relevant investigations for the purposes of preventing and detecting crime or preventing disorder, and to all contractors and external agencies that may be used for this purpose as well as to those members of staff tasked with the authorisation and monitoring of the use of directed surveillance, CHIS and the acquisition of communications data.

It is essential that the Chief Executive and Directors should have an awareness of the basic requirements of RIPA and also an understanding of how it might apply to the work of individual council departments. Without this knowledge at senior level, it is unlikely that any authority will be able to develop satisfactory systems to deal with the legislation. Those who need to use or conduct directed surveillance or CHIS on a regular basis will require more detailed specialised training.

The use of directed surveillance or a CHIS must be necessary and proportionate to the alleged crime or disorder. Usually, it will be considered to be a tool of last resort, to be used only when all other less intrusive means have been used or considered.

Necessary

A person granting an authorisation for directed surveillance must consider *why* it is necessary to use covert surveillance in the investigation *and* believe that the activities to be authorised are necessary on one or more statutory grounds.

If the activities are deemed necessary, the authoriser must also believe that they are proportionate to what is being sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

Proportionate

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 render intrusive 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.

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 reasonably practicable, what other methods had been considered and why they were not implemented.

The Council will conduct its directed surveillance operations in strict compliance with the Data Protection Act (DPA) principles and limit them to the exceptions permitted by the Human Rights Act and RIPA, and solely for the purposes of preventing and detecting crime or preventing disorder.

The **Senior Responsible Officer** (SRO) as named in Appendix 2 will be able to give advice and guidance on this legislation. The SRO will appoint a RIPA Single Point of Contact/Coordinating Officer (SPOC) (as named in Appendix 2). The SPOC will be responsible for the maintenance of a **central register** that will be available for inspection by the Investigatory Powers Commissioner's Office (IPCO).

The use of hand-held cameras and binoculars can greatly assist a directed surveillance operation in public places. However, if they afford the investigator a view into private premises that would not be possible with the naked eye, the surveillance becomes intrusive and is not permitted. Best practice for compliance with evidential rules relating to photographs and

video/CCTV footage is contained in Appendix 4. Directed surveillance may be conducted from private premises. If they are used, the applicant must obtain the owner's permission, in writing, before authorisation is given. If a prosecution then ensues, the applicant's line manager must visit the owner to discuss the implications and obtain written authority for the evidence to be used.

The general usage of the council's CCTV system is not affected by this policy. However, if cameras are specifically targeted for the purpose of directed surveillance, a RIPA authorisation must be obtained.

Wherever knowledge of **confidential information** is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be made by the Chief Executive (or in their absence whoever deputises for this role).

Directed surveillance that is carried out in relation to a **legal consultation** on certain premises will be treated as intrusive surveillance, regardless of whether legal privilege applies or not. These premises include prisons, police stations, courts, tribunals and the premises of a professional legal advisor. Local Authorities are not able to use intrusive surveillance. Operations will only be authorised when there is sufficient, documented, evidence that the alleged crime or disorder exists and when directed surveillance is considered to be a necessary and proportionate step to take in order to secure further evidence.

Low level surveillance, such as 'drive-bys' or everyday activity observed by officers in the course of their normal duties in public places, does not need RIPA authority. If surveillance activity is conducted in immediate response to an unforeseen activity, RIPA authorisation is not required. However, if repeated visits are made for a specific purpose, authorisation may be required. In cases of doubt, legal advice should be taken.

When vehicles are being used for directed surveillance purposes, drivers must at all times comply with relevant traffic legislation.

Crime Threshold

An additional barrier to authorising directed surveillance is set out in the Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012. This provides a 'Crime Threshold' whereby only crimes which are either punishable by a maximum term of at least 6 months' imprisonment (whether on summary conviction or indictment) or are related to the underage sale of alcohol or tobacco can be investigated through Directed Surveillance.

A crime threshold applies to the authorisation of directed surveillance by local authorities under RIPA and the acquisition of Communications Data (CD). It does not apply to the authorisation of local authority use of CHIS.

Thurrock 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 6 months' imprisonment.

Thurrock may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a Magistrate has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial fraud.

Thurrock may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a Justice of the Peace (JP) has been granted.

A local authority such as Thurrock may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences.

An Authorising Officer's Aide-Memoire has been produced (Appendix 6) to assist Authorising Officers when considering applications for directed surveillance

3. Covert Human Intelligence Sources (CHIS)

A person who reports suspicion of an offence is not a CHIS, nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if they establish or maintain a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

If it is deemed unnecessary to obtain RIPA authorisation in relation to the proposed use of a CHIS for test purchasing, the applicant should complete the council's CHIS form and submit to an Authorising Officer for authorisation. Once authorised, any such forms must be kept on the relevant investigation file, in compliance with the Criminal Procedure for Investigations Act 1996 ("CPIA").

The times when a local authority will use a CHIS are limited. The most common usage is for test-purchasing under the supervision of suitably trained officers.

Officers considering the use of a CHIS under the age of 18, and those authorising such activity must be aware of the additional safeguards identified in The Regulation of Investigatory Powers (Juveniles) Order 2000 and its Code of Practice. The most recent order which is SI 2018/715 (http://www.legislation.gov.uk/uksi/2018/715/made)

A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness, and who is or may not be able to take care of himself. The Authorising Officer in such cases must be the Chief Executive, who is the Head of Paid Service, or in their absence whoever deputises for this role.

Any deployment of a CHIS should take into account the safety and welfare of that CHIS. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that an appropriate bespoke risk assessment is carried out to determine the risk to the CHIS of any assignment and the likely consequences should the role of the CHIS become known. This risk assessment must be specific to the case in question. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.

A CHIS handler is responsible for bringing to the attention of a CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect the validity of the risk assessment, the conduct of the CHIS, and the safety and welfare of the CHIS.

The process for applications and authorisations have similarities to those for directed surveillance but there are also significant differences, namely that the following arrangements must be in place at all times in relation to the use of a CHIS:

- There will be an appropriate officer of the Council who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS; and

- There will be a second appropriate officer of the use made of the CHIS, and who will have responsibility for maintaining a record of this use. These records must also include information prescribed by the Regulation of Investigatory Powers (Source Records) Regulations 2000. Any records that disclose the identity of the CHIS must not be available to anyone who does not have a need to access these records.

4. The Authorisation Process

The processes for applications and authorisations for CHIS are similar as for directed surveillance, but note the differences set out in the CHIS section above. Directed Surveillance applications and CHIS applications are made using forms that have been set up in a shared network drive by the council. These forms must not be amended and applications will not be accepted if the approved forms are not completed.

The authorisation process involves the following steps and is also summarised (in flowchart form) within Appendix 7:

Investigation Officer

1. A risk assessment will be conducted by the Investigation Officer before an application is drafted. This assessment will include the number of officers required for the operation; whether the area involved is suitable for directed surveillance; what equipment might be necessary, health and safety concerns of all those involved and affected by the operation and insurance issues. Particular care must be taken when considering surveillance activity close to schools or in other sensitive areas. If it is necessary to conduct surveillance around school premises, the applicant should inform the head teacher of the nature and duration of the proposed activity, in advance. A Police National Computer (PNC) check on those targets should be conducted as part of this assessment by the Counter Fraud & Investigation team.

2. The Investigation Officer prepares an application. When completing the forms, Investigation Officers must fully set out details of the covert activity for which authorisation is sought to enable the Authorising Officer to make an informed judgment. Consideration should be given to consultation with a lawyer concerning the activity to be undertaken (including scripting and tasking).

3. The Investigation Officer will submit the application form to an authorising officer for approval.

4. All applications to conduct directed surveillance (other than under urgency provisions – see below) must be made in writing in the approved format.

Authorising Officer (AO)

5. The AO considers the application and if it is considered complete the application is signed off and forwarded to the Senior Responsible Officer (SRO). It should be noted that the AO is responsible and/or accountable for the authorisation of applications and not the SRO. The SRO role is a quality assurance role (e.g. to ensure the request meets the crime threshold)

6. An Authorising Officer's Aide-Memoire has been produced to assist AO's when considering applications for directed surveillance. This must be completed by the AO.

7. If there are any deficiencies in the application further information may be sought from the Investigation Officer, prior to sign off.

8. Once reviewed by the SRO (see below), the AO and the Investigation Officer will retain copies and will create an appropriate diary method to ensure that any additional documents are submitted in good time.

Senior Responsible Officer (SRO)

9. The SRO then reviews the AO's approval and countersigns it. As referred to above, the AO is responsible and/or accountable for the authorisation of applications and not the SRO. The SRO role is a quality assurance role (e.g. to ensure the request meets the crime threshold)

10. If the application requires amendment the SRO will return this to the AO for the necessary revisions to be made prior to sign off. Once the SRO is satisfied that concludes the internal authorisation procedure and he or she will countersign the application (see section 5 below). This will allow the Investigation Officer to link in with the RIPA Single Point of Contact, in order to obtain a unique reference number (URN) from the central register (prior to any court authorisation).

Application to JPs Court

11. The countersigned application form will form the basis of the application to the JPs Court (see further below).

Authorised Activity

12. Authorisation takes effect from the date and time of the approval from the JPs Court.

13. Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the Counter Fraud & Investigation team.

14. Notification of the operation will be made to the relevant police force intelligence units where the target of the operation is located in their force area. Contact details for each force intelligence unit are held by the Group Manager Counter Fraud & Investigation - Counter Fraud & Investigation team.

15. Before directed surveillance activity commences, the Investigation Officer will brief all those taking part in the operation. The briefing will include details of the roles to be played by each officer, a summary of the alleged offence(s), the name and/or description of the subject of the directed surveillance (if known), a communications check, a plan for discontinuing the operation and an emergency rendezvous point. A copy of the briefing report (Appendix 3) will be retained by the Investigation Officer.

16. Where 3 or more officers are involved in an operation, officers conducting directed surveillance will complete a daily log of activity an example shown at Appendix 5. Evidential notes will also be made in the pocket notebook of all officers engaged in the operation regardless of the number of officers on an operation. These documents will be kept in accordance with the appropriate retention guidelines.

17. Where a contractor or external agency is employed to undertake any investigation on behalf of the Council, the Investigation Officer will ensure that any third party is adequately informed of the extent of the authorisation and how they should exercise their duties under that authorisation.

Conclusion of Activities

18. As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form.

19. The original copy of the complete application will be retained with the central register.

5. Senior Responsible Officer (SRO) Review and Sign Off

The SRO will review the AO approval prior to it being submitted for Magistrates/JP authorisation. This is from a quality assurance aspect only, as the AO has overall responsibility and accountability for signing off applications (and not the SRO).

Once the SRO has countersigned the form this will form the basis of the application to the Magistrates Court for authorisation.

6. Judicial Authorisation

The Authorising Officer or Investigating Officer will provide the court with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the court and should contain all information that is relied upon. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of their consideration.

The original RIPA authorisation or notice should be shown to the court but also be retained by Thurrock Council so that it is available for inspection by the Commissioners' officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The Court may also wish to keep a copy so an extra copy should be made available to the Court.

Importantly, the Authorising Officer or Investigating Officer will also need to provide the court with a partially completed judicial application/order form. The order section of the form will be completed by the JP and will be the official record of the JP's decision.

The officer from Thurrock will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

The authorisation will take effect from the date and time of the JP granting approval and Thurrock may proceed to use the techniques approved in that case.

On the rare occasions where due to out of hours and no access to a Court and Justice of the Peace (JP), then it will be for the officer to make local arrangements with the relevant Her Majesty's Courts and Tribunals Service. In these cases the council will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. They should provide the court with a copy of the signed judicial application/order form the next working day.

In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline.

It is not Thurrock's policy that legally trained personnel are required to make the case to the JP. The forms and supporting papers must by themselves make the case.

7. Authorisation periods

The authorisation will take effect from the date and time of the JP granting approval and Thurrock may proceed to use the techniques approved in that case.

A written authorisation (unless renewed or cancelled) will cease to have effect after 3 months. The Authorising Officer should set a review date at the outset which should be "as frequently as is considered necessary and practicable" (the "norm" is one month after authorisation).

Renewals should not normally be granted more than seven days before the original expiry date. If the circumstances described in the application alter, the applicant must submit a review document before activity continues.

As soon as the operation has obtained the information needed to prove, or disprove, the allegation, the applicant must submit a cancellation document and the authorised activity must cease.

CHIS authorisations will (unless renewed or cancelled) cease to have effect 12 months from the day on which authorisation took effect, except in the case of juvenile CHIS which will cease to have effect after 4 months. Urgent oral authorisations or authorisations will unless renewed, cease to have effect after 72 hours.

8. Urgency

The law has been changed so that urgent cases can no longer be authorised orally. Approval for directed surveillance in an emergency must now be obtained in written form. Oral approvals are no longer permitted. In cases where emergency approval is required an AO must be visited by the applicant with two completed RIPA application forms. The AO will then assess the proportionality, necessity and legality of the application. If the application is approved then the applicant must then contact the out-of-hours HMCTS representative to seek approval from a Magistrate. The applicant must then take two signed RIPA application forms and the judicial approval form to the Magistrate for the hearing to take place.

As with a standard application the test of necessity, proportionality and the crime threshold must be satisfied. A case is not normally to be regarded as urgent unless the delay would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation. Examples of situations where emergency authorisation may be sought would be where there is intelligence to suggest that there is a substantial risk that evidence may be lost, a person suspected of a crime is likely to abscond, further offences are likely to take place and/or assets are being dissipated in a criminal investigation and money laundering offences may be occurring. An authorisation is not considered urgent if the need for authorisation has been neglected or the urgency is due to the authorising officer or applicant's own doing.

9. Communications Data (CD) and the use of the National Anti- Fraud Network (NAFN)

Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Authorising Officers (AO) must not authorise requests for their own service area and will access the restricted area of the National Anti-Fraud Network (NAFN) website using a special code, in order to review and approve the application. When approving the application, the AO must be satisfied that the acquiring of the information is necessary, proportionate and meets the serious crime threshold.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD Code of Practice.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

10. Handling of material and use of material as evidence including retention

Material obtained from properly authorised directed surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of directed surveillance, a source or the obtaining or disclosure of communications data, following relevant legislation such as the Criminal Procedure and Investigations Act (CPIA).

Authorising Officers must ensure compliance with the appropriate data protection and CPIA requirements, having due regard to the Public Interest Immunity test and any relevant Corporate Procedures relating to the handling and storage of material.

Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

The following arrangements are in place to ensure that directed surveillance records are held for as long as necessary:

- For cases resulting in no prosecution, all information/records will be held for 3 years at which point it will be removed/deleted from council systems
- For cases resulting in prosecution, information/records will be held for 7 years at which point the information will be removed/deleted from council systems

- The Records Management Team will ensure that the above is monitored and complied with and this will include the deletion of email related records.

11. Training

Officers conducting directed surveillance operations, using a CHIS or acquiring communications data must have an appropriate accreditation or be otherwise suitably qualified or trained.

Authorising Officers will be appointed by the Chief Executive and will have received training that has been approved by the Senior Responsible Officer. The Senior Responsible Officer will have appointed the RIPA Coordinating Officer (SPOC) who will be responsible for arranging suitable training for those conducting surveillance activity or using a CHIS.

All training will take place at reasonable intervals to be determined by the SRO or SPOC, but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

12. Surveillance Equipment

All mobile surveillance equipment is kept in secure premises of each investigation and enforcement team in the Civic Offices. Access to the area is controlled by the relevant team, who maintain a spreadsheet log of all equipment taken from and returned to the area.

13. The Inspection Process

The Investigatory Powers Commissioners Office (IPCO) will make periodic inspections during which the inspector will wish to interview a sample of key personnel; examine RIPA and CHIS applications and authorisations; the central register and policy documents. The inspector will also make an evaluation of processes and procedures.

14. Shared Arrangements

Thurrock conducts Counter Fraud & Investigation activities to protect other public authorities who have no counter fraud function but have an ongoing statutory duty to protect the public funds they administer. In rare instances, where activity governed by RIPA is required to support that Counter Fraud work, only officers employed by Thurrock Council are used to conduct that activity, as the tasking agency. Thurrock therefore follows its own RIPA policy which will result in its Authorising Officers' signing off other agencies RIPA surveillance requests.

15. Social Media and online covert activity

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Alternatively an investigator may need to communicate covertly online, for example, contacting individuals using social media websites.

Whenever the council intends to use the internet as part of an investigation, it must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights (Right to respect for private and family life), including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case.

The use of social media for the gathering of evidence to assist in enforcement activities, must comply with the requirements set out below:

- It is not unlawful for a council officer to set up a false identity but it is inadvisable to do so for a covert purpose without authorization. If this is being considered then this must be authorised by the Senior Responsible Officer and/or the RIPA Single Point of Contact. Using photographs of other persons without their permission to support the false identity infringes other laws.
- Where it is necessary and proportionate for officers pursuing an investigation to create a false identity in order to 'friend' individuals on social networks, a CHIS authorisation must be obtained.
- Authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a council officer (i.e. the activity is more than merely reading of the site's content). Where activity is only carrying out a test purchase a CHIS authorisation may not be necessary, however this should be confirmed with the Authorising Officer on a case by case basis.
- Where privacy settings are available but not applied, the data may be considered open source and an authorisation is not usually required. However privacy implications may still apply even if the subject has not applied privacy settings (see section 3.13 of the Covert Surveillance and Property Interference Code). Advice on this must be obtained from the Senior Responsible Officer and/or the RIPA Single Point of Contact prior to undertaking surveillance.
- Officers viewing an individual's open profile on a social network should do so as infrequently as possible in order to substantiate or refute an allegation.
- Where repeated viewing of open profiles on social networks is necessary and proportionate to gather further evidence or to monitor an individual's status, then RIPA authorisation must be considered as repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis. Any decision not to seek authorisation must be made in consultation with an Authorising Officer and that the decision making process should be documented.
- 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, then reasonable steps must be undertaken to ensure its validity

Please note, sections 3.10 through to 3.17 of the Surveillance and Property Interference Code (and 4.11 to 4.17 of the CHIS Code) provide detailed information in relation to this subject matter.

Based on the above:

- All online activity conducted in connection with children's services, enforcement or investigative functions, must be recorded and periodically scrutinised for oversight purposes
- Records of visits by staff to any social media sites must be documented by staff at all times. An example log is shown below (referred to as a Social Media Activity Log)
- The RIPA Single Point of Contact will ensure that service areas are contacted on a quarterly basis, to establish if any on-line activity has been undertaken and if so request the return of the relevant Social Media Activity Logs

Social Media Activity Log:

Date of Monitoring	**Name of individual who is the subject of the monitoring**	**Reason for the monitoring**	**Was the monitoring a one-off exercise? If not has a directed surveillance request been approved**
15/01/2021	Alan Smith	To undertake checks to establish a child's attendance at school	Yes it was a one-off exercise with no additional checks/monitoring required

Appendix 1

GLOSSARY OF TERMS

Collateral intrusion
The likelihood of obtaining private information about someone who is not the subject of the directed surveillance operation.

Confidential information
This covers confidential journalistic material, matters subject to legal privilege, and information relating to a person (living or dead) relating to their physical or mental health; spiritual counselling or which has been acquired or created in the course of a trade/profession/occupation or for the purposes of any paid/unpaid office.

Covert relationship
A relationship in which one side is unaware of the purpose for which the relationship is being conducted by the other.

Directed Surveillance
Surveillance carried out in relation to a specific operation which is likely to result in obtaining private information about a person in a way that they are unaware that it is happening. It excludes surveillance of anything taking part in residential premises or in any private vehicle.

Intrusive Surveillance
Surveillance which takes place on any residential premises or in any private vehicle. A Local Authority cannot use intrusive surveillance.

Legal Consultation
A consultation between a professional legal adviser and his client or any person representing his client, or a consultation between a professional legal adviser or his client or representative and a medical practitioner made in relation to current or future legal proceedings.

Residential premises
Any premises occupied by any person as residential or living accommodation, excluding common areas to such premises, e.g. stairwells and communal entrance halls.

Senior Responsible Officer (SRO)
The SRO is responsible for the integrity of the processes in order for the Council to ensure compliance when using Directed Surveillance or CHIS.

Service data
Data held by a communications service provider relating to a customer's use of their service, including dates of provision of service; records of activity such as calls made, recorded delivery records and top-ups for pre-paid mobile phones.

Surveillance device
Anything designed or adapted for surveillance purposes.

Appendix 2

List of Authorising Officers

Principal RIPA Officers

Ian Hunt Assistant Director of Law and Governance & Monitoring Officer	Senior Responsible Officer (SRO)
Matthew Boulter Deputy Monitoring Officer	Deputy SRO
Lee Henley Strategic Lead -Information Management	RIPA Co-ordinating Officer (Single Point of Contact)

Authorising Officers

Chief Executive	Authorising Officer
Sean Clark Director of Finance & IT	Authorising Officer
Andrew Millard Director of Place	Authorising Officer
Jackie Hinchliffe Director of HR,OD & Transformation	Authorising Officer
Julie Rogers Director Environment and Highways	Authorising Officer

Appendix 3

Briefing Report

Before any RIPA or CHIS operation commences, all staff will be briefed by the officer in charge of the case using the format of this briefing report. The original will be retained with the investigation file.

RIPA URN ……

Name and number to identify operation …….

Date, time and location of briefing ……..

……

Persons present at briefing ……..

……

Information (Sufficient background information of the investigation to date to enable all those taking part in the operation to fully understand their role).

Intention (What is the operation seeking to achieve?).

Method (How will individuals achieve this? If camcorders are to be used, remind officers that any conversations close to the camera will be recorded).

Administration (To include details of who will be responsible for maintenance of the log sheet and collection of evidence; any identified health and safety issues; the operation; an agreed stand down procedure – NOTE It will be the responsibility of the officer in charge of the investigation to determine if and when an operation should be discontinued due to reasons of safety or cost-effectiveness – and an emergency rendezvous point. On mobile surveillance operations, all those involved will be reminded that at ALL times speed limits and mandatory road signs MUST be complied with and that drivers must NOT use radios or telephones when driving unless the equipment is 'hands free').

Communications (Effective communications between all members of the team will be established before the operation commences).

Appendix 4

Best practice regarding photographic and video evidence

Photographic or video evidence can be used to support the verbal evidence of what the officer conducting surveillance actually saw. There will also be occasions when video footage may be obtained without an officer being present at the scene. However it is obtained, it must properly documented and retained in order to ensure evidential continuity. All such material will be disclosable in the event that a prosecution ensues.

Considerations should be given as to how the evidence will eventually be produced. This may require photographs to be developed by an outside laboratory. Arrangements should be made in advance to ensure continuity of evidence at all stages of its production. A new film, tape or memory card should be used for each operation.
If video footage is to be used start it with a verbal introduction to include day, date, time and place and names of officers present. Try to include footage of the location, e.g. street name or other landmark so as to place the subject of the surveillance.

A record should be maintained to include the following points:

- Details of the equipment used
- Confirmation that the date & time on the equipment is correct
- Name of the officer who inserted the film, tape or memory card into the camera
- Details of anyone else to whom the camera may have been passed
- Name of officer removing film, tape or memory card
- Statement to cover the collection, storage and movement of the film, tape or memory card
- Statement from the person who developed or created the material to be used as evidence

As soon as possible the original recording should be copied and the master retained securely as an exhibit. If the master is a tape, the record protect tab should be removed once the tape has been copied. Do not edit anything from the master. If using tapes, only copy on a machine that is known to be working properly. Failure to do so may result in damage to the master.

Stills may be taken from video. They are a useful addition to the video evidence.

Appendix 5

Surveillance Log

Daily log of activity, to be kept by each operator or pair of operators.

A – Amount of time under observation
D – Distance from subject
V - Visibility
O - Obstruction
K – Known, or seen before
A – Any reason to remember, subject or incident
T – Time elapsed between sighting and note taking
E – Error or material discrepancy – e.g. description, vehicle reg etc.

Operation name or number …….

Date ……..……..

Time of activity (from) ……..….. (to) …….

Briefing location and time …….

Name of operator(s) relating to THIS log …….

…….

Details of what was seen, to include ADVOKATE (as above).

…….

…….

…….

…….

…….

…….

…….

Appendix 6

RIPA Authorising Officer's Aide-Memoire

Has the applicant satisfactorily demonstrated proportionality? Court will ask itself should (not could) we have decided this was proportionate. Is there a less intrusive means of obtaining the **same** information? What is the risk – to the authority (loss), to the community of allowing the offence to go un-investigated? What is the potential risk to the subject? What is the least intrusive way of conducting the surveillance? Has the applicant asked for too much? Can it safely be limited? Remember – Don't use a sledge-hammer to crack a nut! YOUR COMMENTS	**Yes**	**No**

Has the applicant satisfactorily demonstrated necessity (see below)? • What crime is alleged to being committed? • Is the surveillance necessary for what we are seeking to achieve? • Does the activity need to be covert or could the objectives be achieved overtly? • Does this crime come under the Fraud Act 2006 and if so please state which section of the Act this applies to? • Will the offence attract a custodial sentence of 6 months or more? If no, directed surveillance should not be used YOUR COMMENTS	**Yes**	**No**

What evidence does applicant expect to gather? Has applicant described (a) what evidence he/she hopes to gain, and (b) the value of that evidence in relation to THIS enquiry? YOUR COMMENTS	**Yes**	**No**

Is there any likelihood of obtaining confidential information during this operation? If "Yes" operation must be authorized by the Chiel Executive.	**Yes**	**No**
Have any necessary risk assessments been conducted before requesting authorization? Details what assessment (if any) was needed in this particular cases. In the case of a CHIS authorization an appropriate bespoke risj assessment must be completed.	**Yes**	**No**
When applying for **CHIS** authorization, have officers been identified to: a) have day to day responsibility for the CHIS (a handler) b) have general oversight of the use of the CHIS (a controller) c) be responsible for retaining relevant CHIS records, including true identity, and the use made of the CHIS.	**Yes**	**No**

Have all conditions necessary for authorization been met to your satisfaction? GIVE DETAILS	**Yes**	**No**

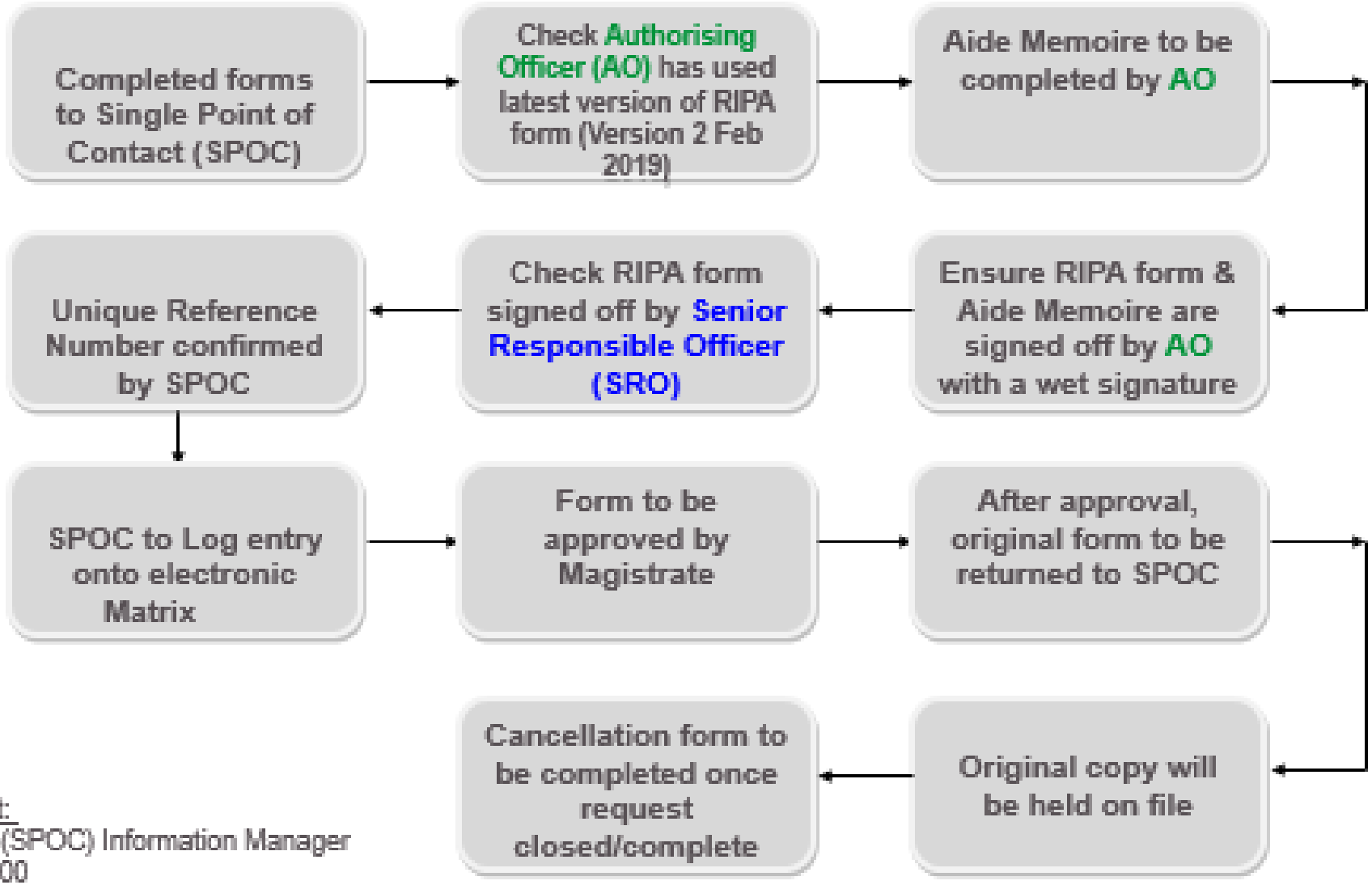
Do you consider that it is necessary to place limits on the operation? IF YES, GIVE DETAILS (e.g. no. of officers, time, date etc.) and REAASONS	**Yes**	**No**

Name (Print)		Grade / Rank		
Signature		Date and time		
Expiry date and time [e.g.: authorisation granted on 1 April 2011 - expires on 30 June 2011, 23.59]				

Remember to diarise any review dates and any subsequent action necessary by you and/or applicant. Return copy of completed application to applicant and submit original to Legal Services. Retain copy.

RIPA Process

Appendix 7



Key Contact:
Lee Henley (SPOC) Information Manager
01375 652500