REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) CORPORATE POLICY

USE OF DIRECTED SURVEILLANCE COVERT HUMAN INTELLIGENCE SOURCES AND COMMUNICATIONS DATA ACQUISITION FOR THE PREVENTION AND DETECTION OF CRIME OR THE PREVENTION OF DISORDER

Version 7 – draft – January 2014

Contents

Appendices

29.	Appendix 11a – CHIS application form	
30.	Appendix 11b – CHIS review form	
31.	Appendix 11c – CHIS renewal form	
32.	Appendix 11d – CHIS cancellation form 52 Appendix 11e – Authorisation form for test purchasing	
33.	Appendix 12 – R v Johnson (Kenneth) 1988 1 WLR 1377 CA	
34.	Appendix 13 – RIPA Authorising Officer's Aide-Memoire	
35.	Appendix 14 – RIPA Authorisation Quarterly Audit Record	

1. A BRIEF OVERVIEW OF RIPA

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

The Regulation of Investigatory Powers Act (the Act) 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 authorized.

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 RIP (Directed Surveillance and CHIS)(Amendment) Order 2012 (Appendix 2).

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) (Appendix 3), and the Data Protection Act (DPA) (Appendix 4).

The purpose of Part II of the Act is to protect the privacy rights of anyone in a Council's area, but only to the extent that those rights are protected by the HRA. A public authority, such as the Council, has the ability to infringe those rights provided that it does so in accordance with the rules, which are contained within Part II of the Act. Should the public authority not follow the rules, the authority looses the impunity otherwise available to it. This impunity may be a defence to a claim for damages or a complaint to supervisory bodies, or as an answer to a challenge to the admissibility of evidence in a trial.

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 behaviour 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;
- Benefits fraud – investigating 'living together' and 'working whilst in receipt of benefit' allegations and council tax evasion; 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.
The RIPA (Communications Data) order came into force in 2004. It allows Local Authorities to acquire communications data, namely service data and subscriber details for limited purposes. This order was updated by the Regulation of Investigatory Powers Communications Data) Order 2010.

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.

The policy will be reviewed annually and whenever changes are made to relevant legislation and codes of practice.

'It is essential that the Chief Executive, or Head of Paid Service, together with the Directors and the Heads of Units 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' (Office of Surveillance Commissioners).

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 DPA principles and limit them to the exceptions permitted by the HRA and RIPA, and solely for the purposes of preventing and detecting crime or preventing disorder.

The **Senior Responsible Officer** (SRO) (as named in Appendix 5) will be able to give advice and guidance on this legislation. The SRO will appoint a **RIPA Coordinating Officer** (RCO) (as named in Appendix 5) The RCO will be responsible for the maintenance of a **central register** that will be available for inspection by the Office of the Surveillance Commissioners (OSC). The format of the central register is set out in Appendix 7.

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 9. 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. (See R v Johnson (Kenneth) 1988 1 WLR 1377 CA. Appendix 29)

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, who is the Head of Paid Service (or in his absence whoever deputises for him).

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.

The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold came into effect on 1 November 2012.

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 benefit 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 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

3. 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 form provided at Appendix 11e and submit to the Head of Public Protection for authorisation. Once authorised, any such forms must be kept on the relevant Trading Standards file.

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

For some test purchases it will be necessary to use a CHIS who is, or appears to be, under the age of 16 (a juvenile). Written parental consent for the use of a juvenile CHIS must be obtained prior to authorisation, and the duration of such an authorisation is 1 month instead of the usual 12 months. The Authorising Officer must be the Chief Executive or Deputy. NOTE: A juvenile CHIS may not be used to obtain information about their parent or guardian.

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.

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 his absence whoever deputises for him.

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 (see Appendices 11a-11d), 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:

1. 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

2. 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.

An Authorising Officer's Aide-Memoire is provided at Appendix 13 to assist Authorising Officers when considering applications for directed surveillance.

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 are made using forms in Appendix 6 and CHIS applications are made using forms at Appendices 11a-11d.

The authorisation process involves the following steps:

Investigation Officer

1. 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.

2. The Investigation Officer will obtain a unique reference number (URN) from the central register before submitting an application.

3. A risk assessment will be conducted by the Investigation Officer within 7 days of the proposed start date. 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 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.

4. The Investigation Officer will submit the application form to an authorising officer for approval (see Appendix 5).

5. 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)

6. The AO considers the application and if it is considered complete the application is signed off and forwarded to the SRO for review and counter approval.

7. An Authorising Officer's Aide-Memoire is provided at Appendix 13 to assist Authorising Officers when considering applications for directed surveillance.

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

9. Once final approval has been received from 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)

10. The SRO then reviews the AO's approval and countersigns it.

11. 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.

Application to Magistrates Court

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

Authorised Activity

13. Authorisation takes effect from the date and time of the approval from the Magistrates Court.

14. Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the DVLA.

15. 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 is held by the Fraud Investigation Manager - Fraud Investigation Department.

16. 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 8) will be retained by the Investigation Officer.

17. Where 3 or more officers are involved in an operation, officers conducting directed surveillance will complete a daily log of activity as at Appendix 10. 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.

18. 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

19. As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form (Appendices 6d or 11d).

20. The original document of the complete application will be retained with the central register.

5. SRO Review and Sign Off

The SRO will review the AO approval prior to it being submitted for Magistrates/JP authorisation.

If in the SRO's opinion there are inconsistencies, errors or deficiencies, in the application such that the AO's approval requires amendments or augmentation, the SRO will return the application form to the AO with recommendation for alternative wording or further information and the AO will incorporate the same.

The form will then be returned to the SRO for countersigning.

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

6. Magistrate Authorisation

From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 are in force. This will mean that a local authority who wishes to authorise the use of directed surveillance, acquisition of CD and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

The new judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined above and in this section. The current process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will therefore remain the same.

The appropriate officer from Thurrock will provide the JP 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 JP and should contain all information that is relied upon. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration.

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

Importantly, the appropriate officer will also need to provide the JP with a partially completed judicial application/order form.

Although the officer is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

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.

It will be important for each officer seeking authorisation to establish contact with HMCTS administration at the magistrates' court. HMCTS administration will be the first point of contact for the officer when seeking a JP approval. Thurrock will need to inform HMCTS administration as soon as possible to request a hearing for this stage of the authorisation.

On the rare occasions where out of hours access to a JP is required then it will be for the officer to make local arrangements with the relevant HMCTS legal staff. In these cases we 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. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.
The hearing is a 'legal proceeding' and therefore our officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.

The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

The attending officer will need to be able to answer the JP's questions on the policy and practice of conducting covert operations and the detail of the case itself. Thurrock's officers may consider it appropriate for the SPoC (single point of contact) to attend for applications for CD RIPA authorisations. This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered and which are provided to the JP to make the case (see paragraphs 47-48).

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. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the form any additional information he or she has received during

the course of the hearing but information fundamental to the case should not be submitted in this manner.

If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

The JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely. Magistrates' courts are not public authorities for the purposes of the Freedom of Information Act 2000.

Thurrock will need to provide a copy of the order to the communications the SPoC (Single Point of Contact) for all CD requests. SPoCs must not acquire the CD requested, either via the CSP or automated systems until the JP has signed the order approving the grant.

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. Urgent oral or written authorisations, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

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 1 month. 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 judgement 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. Telecommunications Data - NAFN

The RIPA (Communications Data) Order 2003 came into law in January 2004. It allows Local Authorities to acquire limited information in respect of subscriber details and service data. It does NOT allow Local Authorities to intercept record or otherwise monitor communications data.

Applications to use this legalisation must be submitted to a Home Office accredited Single Point of Contact (SPOC). The Council uses the services of NAFN (the National Anti-fraud Network) for this purpose.

Officers may make the application by accessing the NAFN website. The application will first be vetted by NAFN for consistency, before being forwarded by NAFN to the Council's Designated Persons for the purposes of approving the online application. The Council will ensure that Designated Persons receive appropriate training when becoming a Designated Person.

The Council's Designated Persons are presently the relevant Heads of Service, CEO and the Council's Monitoring Officer. NAFN will inform the Designated Persons jointly once the application is ready to be reviewed by the Designated Persons.

The relevant Designated Persons responsible for the area to which the application relates, will then access the restricted area of the NAFN website using a special code, in order to review and approve the application. When approving the application, the Designated Person must be satisfied that the acquiring of the information is necessary and proportionate. Approvals are documented by the Designated Person completing the online document and resubmitting it by following the steps outlined on the site by NAFN. This online documentation is retained by NAFN who are inspected and audited by the OSC.

When submitting an online application, the officer must also inform the relevant Designated Person, in order that they are aware that the NAFN application is pending.

10. Handling of material and use of material as evidence

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. Authorising Officers must ensure compliance with the appropriate data protection requirements 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.

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 (Appendix 5) 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 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 RSO, 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 a secure area on the second floor of the Civic Offices. Access to the area is controlled by the Community Protection Team, who maintains a spreadsheet log of all equipment taken from and returned to the area.

13. RIPA Record Audits

To ensure directed surveillance authorisations are being conducted in accordance with Council policy, a system of internal quality assurance has been put in place. At quarterly periods throughout the year, Directors acting in their capacity of authorising officers will in turn conduct an audit of the RIPA records pertaining to the previous 3 months. The audit must be recorded on the audit record form to be found at Appendix 14, and a copy submitted to the Senior Responsible Officer to be held centrally on file. The Senior Responsible Officer will inform the Chief Executive of the outcome of such audits.

14. The Inspection Process

The OSC 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.

15. Resources

Full Codes of Practice can be found on the Home Office website: http://www.homeoffice.gov.uk/

Covert Surveillance & Property Interference: https://www.gov.uk/government/publications/code-of-practice-for-covert-surveillance-and-property-interference

CHIS: https://www.gov.uk/government/publications/code-of-practice-for-the-use-of-human-intelligence-sources

Acquisition and Disclosure of Communications Data: https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

Further information can also be found on The Office of Surveillance Commissioners website. http://www.surveillancecommissioners.gov.uk/index.html

Appendix 1

GLOSSARY OF TERMS

(For full definitions, refer to the Act)

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.

RIPA Coordinating Officer (RCO)

Is the officer appointed by the SRO to coordinate the ongoing internal procedures for compliance when using Directed Surveillance or CHIS. This includes maintaining the Central Register, arranging training and coordinating information for audits and inspections.

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

Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

The Order consolidates four previous Orders relating to directed surveillance and the use or conduct of covert human intelligence sources by public authorities under Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) and to reflect the outcome of a public consultation which took place between April and July 2009.

It identifies the 'relevant public authorities' authorised to conduct RIPA and CHIS activities. This list includes local authorities in England and Wales. It also gives examples of such activity, as shown on page 3 of this document.

Appendix 3 The Human Rights Act 1998

Articles 6 and 8 of the Human Rights Act are relevant to RIPA.

Article 6 creates the right to a fair trial including fairness in the way that evidence is gathered. Article 6 creates the right to respect for ones private and family life, home and correspondence. These are not absolute rights, but there should be no interference with them, except as is allowed by other statute, such as RIPA.

If it is proposed that directed surveillance evidence is to be used in a prosecution, or other form of sanction, the subject of the surveillance should be informed during an interview under caution.

Appendix 4 The Data Protection Act 1998 (DPA)

The eight principles of the Act relating to the acquisition of personal data need to be observed when using RIPA. To ensure compliance, the information must:

- Be fairly and lawfully obtained and processed
- Be processed for specified purposes only
- Be adequate, relevant and not excessive
- Be accurate
- Not be kept for longer than is necessary
- Be processed in accordance with an individuals rights
- Be secure
- Not be transferred to non EEA countries without adequate protection.

Appendix 5 List of Authorising Officers

6.1 The following post holders may authorise RIPA applications where there is a likelihood of obtaining Confidential Information: Chief Executive or deputy.

6.2 The following post holders may authorise the use of a vulnerable person or a juvenile to be used as a Covert Human Intelligence Source: Chief Executive, as Head of Paid Service or his or her deputy.

6.3 The following post holders may authorise applications, reviews, renewals and cancellations of Directed Covert Surveillance of Covert Human Intelligence Sources: Chief Executives and Directors, or in their absence, the Head of Legal and Democratic Services.

Principal RIPA Officers

Fiona Taylor Head of Legal Services	Senior Responsible Officer (SRO)	01375 652442
Lee Henley Information Manager	RIPA Co-ordinating Officer	01375 652500

Authorising Officers

Graham Farrent Chief Executive	Authorising Officer	01375 652390
 Director of Environment	Authorising Officer	01375 652914
Sean Clark Head of Corporate Finance & s151 Officer	Authorising Officer	01375 652010
Fiona Taylor	Authorising Officer	01365652442

Appendix 6a

RIPA application form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority (including full address)			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation /Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No. 521. [1]
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• Name: • Address: • DOB: • Other information as appropriate:

1 For local authorities: The exact position of the authorising officer should be given.

Unique Reference Number	

5.	Explain the information that it is desired to obtain as a result of the directed surveillance.

6.	Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA.
•	Pursuant to SI 2010, No. 521 Local Authorities can only rely on the following ground: For the purpose of preventing or detecting crime or of preventing disorder;

7.	Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3]

8.	Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11] Describe precautions you will take to minimise collateral intrusion

Unique Reference Number	

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 3.4 – 3.7]

10. Confidential information. [Code paragraphs 4.1 to 4.31] Indicate the likelihood of acquiring any confidential information:

11. Applicant's Details.			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]
I hereby authorise directed surveillance defined as follows: [Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]

Unique Reference Number	

13. Explain why you believe the directed surveillance is necessary. [Code paragraph 3.3] Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 3.4 – 3.7]
14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31

Unique Reference Number	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
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]				
15. Urgent Authorisation [Code paragraphs 5.5 and 5.6]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.				
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer				
Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June			
SRO Sign-off Name (Print)	**Confirmation that SRO has read and approved the application detailed above**	**Date and Time**	**Signature**	

Appendix 6b

RIPA review form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(including address)*	

Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
Details of review:		**Review Number**	

1. Review number and dates of any previous reviews.	
Review Number	**Date**

Unique Reference Number	

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

Unique Reference Number	

7. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].
Name (Print) Grade / Rank ----------Signature ----------Date ----------

10. Date of next review.	

Appendix 6c

RIPA renewal form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Author-ity (including full	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/ Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

Unique Reference Number	

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

Unique Reference Number	

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

s. This box must be completed.

9. Authorising Officer's Statement.
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.
Name (Print) Grade / Rank ----------Signature ----------Date ----------
Renewal From: Time: Date:

Date of first review.	
Date of subsequent reviews of this authorisation.	

Appendix 6d

RIPA cancellation form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority (including full address)	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/ Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

Unique Reference Number	

2. Explain the value of surveillance in the operation:

3. What product has been obtained as a result of the surveillance activity? (You should list here the dates and times of the activity; the nature of the product (i.e., what it shows) and its format (e.g., visual recordings; still images); associated log/reference numbers; where the product is to be held; and the name of the officer responsible for its future management.) **nb** – if you have already provided these details in earlier reviews, a crossreference here should suffice.

Dates/times	Product obtained	Format and reference numbers	Storage location	Officer responsible

4. Authorising Officer's comments on product obtained. (Paragraph 9.3 of the Covert Surveillance Code of Practice states that arrangements must be in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material. **You should record here how you intend this to be achieved**.)

Unique Reference Number	

5. Authorising Officer's comments on the outcome of this use of directed surveillance and formal cancellation instructions.
Name (Print) Grade Signature Date and Time

6. Time and Date when the Authorising Officer instructed the surveillance to cease (if done verbally prior to this formal written cancellation).			
Date:		**Time:**	

Appendix 7

Central Register

A central register will be maintained by Legal and Democratic Services. The register will contain details of all RIPA and CHIS applications (whether approved or not) and all reviews, renewals and cancellations.

Each operation will be given a unique reference number (URN) from which the department involved and the year of the operation may be readily identified.

The register will also contain the following information:

- The operation reference name or number
- The name of the applicant
- The name of the subject of the surveillance or CHIS activity (for internal enquiries a pseudonym may be used)
- The date and time that the activity was authorised
- The date and time of any reviews that are to be conducted
- The date and time of any renewals of authorisations
- The date and time of the cancellations of any authorisations

Kept in conjunction with the register will be details of the training and updates delivered to authorising officers, a list of authorising officers, a copy of the RIPA policy and copies of all relevant legislation.

The original of all documents will also be held with the register, which must be available for inspection by the Office of the Surveillance Commissioners.

Appendix 8

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 or 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 the intention? 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; confirmation that Essex Police have been informed of the locations and times of 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 directed 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 9

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
- 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.

. Appendix 10

Directed Surveillance Log

Daily log of activity, to be kept by each operator where 3 or more officers are involved in the operation.
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 making E – Error or material discrepancy –

e.g. description, vehicle reg. etc.. Operation name or number…….

Date……. Times 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).

……

……

……

……

……

……

……

……

……

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

Appendix 11a

CHIS application form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for authorisation of the conduct for use of a Covert Human Intelligence Source (CHIS)

Public Authority (including full address)			
Name of Applicant		**Service/Department /Branch**	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number			
The name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare. (Often referred to as the Handler)			
The name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source. (Often referred to as the Controller)			
Who will be responsible for retaining (in secure, strictly controlled conditions, with needtoknow access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?			
Investigation/Operation Name (if applicable)			

Unique Reference Number	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No. 521. [2]
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the purpose for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or how the source is to be used.

[2] For local authorities: The exact position of the authorising officer should be given.

Unique Reference Number	

5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA.	
• Pursuant to SI 2010, No. 521 Local Authorities can only rely on the following ground: For the purpose of preventing or detecting crime or of preventing disorder;	
6. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 3.2]	
7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11] Describe precautions you will take to minimise collateral intrusion and how any will be managed.	
8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source? (see Code 3.17 – 3.18)	

Unique Reference Number	

9. Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 6.14 – 6.16)
10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code paragraph 3.3 – 3.5]
11. Confidential information. [Code paragraphs 4.1 to 4.21] Indicate the likelihood of acquiring any confidential information.
References for any other linked authorisations:

12. Applicant's Details.			
Name (print)		**Grade/Rank/Position**	
Signature		**Tel No:**	
Date			

Unique Reference Number	

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.
14. Explain why you believe the conduct or use of the source is necessary. [Code paragraph 3.2]. Explain why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement. [Code paragraph 3.3 – 3.5]
15. (Confidential Information Authorisation.) Supply details demonstrating compliance with Code paragraphs 4.1 to 4.21

16. Date of first review:	

Unique Reference Number	

17. Programme for subsequent reviews of this authorisation: [Code paragraphs 5.15 – 5.16]. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.			
18. Authorising Officer's Details			
Name (Print)		**Grade/Rank/Position**	
Signature		Time and date granted* Time and date authorisation ends	

*** Remember, an authorisation must be granted for a 12 month period**

19. Urgent Authorisation [Code paragraphs 5.13 – 5.14]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.
20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer
21. Authorising Officer of urgent authorisation

Name (Print)		**Grade/Rank/Position**		
Signature		**Date and Time**		
Urgent authorisation expiry date:		**Expiry time:**		

Remember the 72 hour rule for urgent authorisations – check Code of Practice [Code Paragraph 5.14]. e.g. authorisation granted at 1700 on 1st June 2011 expires 1659 on 4th June 2011

Appendix 11b

CHIS review form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Review of a Covert Human Intelligence Source (CHIS) authorisation

Public Authority *(including full address)*	

Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

Unique Reference Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	**Date**
2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.	

3. Det Source **the reasons why it is necessary to continue with using a Covert Human Intelligence Source.**

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Det collate **any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions g.**

Unique Reference Number	

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Give details of the review of the risk assessment on the security and welfare of using the source.

8. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

9. Review Officer's should continue?	**Comments, including whether or not the use or conduct of the source**

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

Name (Print) Grade / Rank Signature Date	
Date of next review:	

Appendix 11c

CHIS renewal form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation

(Please attach the original authorisation)

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

Unique Reference Number	

2. Det it appli	any significant changes to the information as listed in the original authorisation as it applies at the he renewal.

3. Detail why it is necessary t continu with the authorisation, including details of any tasking given to the source. o e

4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.

Unique Reference Number	

7. Detail the results of regular reviews of the use of the source.

8. Give details of the review of the risk assessment on the security and welfare of using the source.

9. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

10. Authorising Officer's Comments. This box must be completed.

11. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY

Unique Reference Number	

Name (Print)	**Grade / Rank**
Signature	**Date**
Renewal From: Time:	**Date:**
NB. Renewal takes effect at the time/date of the original authorisation would have ceased but for the renewal	**End date/time of the**

Date of first review:	
Date of subsequent reviews of this authorisation:	

Appendix 11a

CHIS cancellation form

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Cancellation of an authorisation for the use or conduct of a Covert Human Intelligence Source

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			

n:

1. Explain the reason(s) for the cancellation of the authorisation:

Unique Reference Number	

2. Explain the value of the source in the operation:

3. What product has been obtained as a result of the surveillance activity? (You should list here the dates and times of the activity; the nature of the product (i.e., what it shows) and its format (e.g., visual recordings; still images); associated log/reference numbers; where the product is to be held; and the name of the officer responsible for its future management.) **nb** – if you have already provided these details in earlier reviews, a crossreference here should suffice.

Dates/times	Product obtained	Format and reference numbers	Storage location	Officer responsible

4. Authorising Officer's comments on product obtained. (Paragraph 8.1 of the Covert Human Intelligence Sources Code of Practice states that arrangements must be in place for the handling, storage and destruction of material obtained through the use or conduct of a CHIS. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material. **You should record here how you intend this to be achieved**.)

5. Authorising Officer's comments on the outcome of this use of directed surveillance and formal cancellation instructions.

Unique Reference Number	

Name (Print)	----------	**Grade**	----------
Signature	----------	**Date and Time**	----------

6. Time and Date when the Authorising Officer instructed the surveillance to cease (if done verbally prior to this formal written cancellation).			
Date:		**Time:**	

Appendix 11e

Authorisation Form for Test Purchasing

This is to authorise the following volunteer(s):

1.

2.

3. to attempt to purchase alcohol under the supervision of Trading Standards Officers:

1.

2.

3. on ……201... No Regulation of Investigatory Powers Act (RIPA) authorisation is required for this test

purchase operation, based on the following: Human Rights Act 1988, Schedule 1,

Article 8 -No human rights are being infringed. No private information about any person

is likely to be obtained. There is no intention to establish or maintain a personal or other

relationship with the
seller or any other person.

Signed…….

Name……...
Inspector of Weights and Measures
Trading Standards Thurrock Borough
Council Civic Offices New Road
Grays RM17 6SL

Dated this day ……. 201…

Appendix 12

R v Johnson

R. v. Johnson [1988] 1 WLR 1377 laid down the correct procedure when using observation posts:

- The police officer in charge of the observation, who should be of no lesser rank than sergeant, should testify that he had visited the observation posts & ascertained the attitude of the occupiers to the use of the premises & to disclosure which might lead to their identification. (It is suggested that 'sergeant' could be replaced by section manager).
- An inspector should then testify that immediately before the trial he visited those places & ascertained whether the occupiers were the same persons as those at the time of the observations. (It is suggested that 'inspector' could be replaced by head of department).
- If they were not he, should testify as to their attitude to the use made of the premises and to possible disclosure which might lead to their identification.
- The judge should explain to the jury when summing up or at some other point the effect of his ruling to exclude the evidence of the location.

Public Interest Immunity (PII) protects the identity of a person who has permitted directed surveillance to be conducted from private premise, so this extends to the address and any other information that could reveal their identity. If, however, the location can be revealed without identifying the occupier, then it should be.

Appendix 13

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? *What crime is alleged to be being committed? Has the applicant described it in full?* Is surveillance necessary for what we are seeking to achieve? *Does the activity need to be covert, or could the objectives be achieved overtly?* *YOUR COMMENTS*	Yes	No

Has action been taken to identify and minimise collateral intrusion? Has the applicant identified and described the possible collateral intrusion in all aspects of the operation? Has the applicant shown that consideration has been given to removing/reducing likelihood of collateral intrusion? Could more be done to limit/remove likelihood? *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 authorised by the Chief Executive.	Yes	No
Have any necessary risk assessments been conducted before requesting authorisation? Detail what assessment (if any) was needed in this particular cases. In the case of a CHIS authorisation an appropriate bespoke risk assessment must be completed	Yes	No
When applying for **CHIS** authorisation, 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 authorisation been met to your satisfaction? GIVE DETAILS	Yes	No

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.

Appendix 14

RIPA Authorisation Quarterly Record Audit

ID Number	
Type of Application	
Authorising Officer	
Date of Audit	

Operation / Subject Name	
Lead Officer	
Auditing Officer	

Is the application documented appropriately on the correct form and authorised?	Yes	No

Does the application satisfactorily demonstrate proportionality? *Was there a less intrusive means of obtaining the **same** information?* *What was the risk – to the authority (loss), to the community of allowing the offence to go un investigated? What was the potential risk to the subject?* *Was this the least intrusive way of conducting the surveillance?* *If the applicant asked for too much, has it been appropriately limited?* *YOUR COMMENTS*	Yes	No

Does the application satisfactorily demonstrate necessity? *What crime was alleged to be have been committed? Did the applicant describe it in full?* Was surveillance necessary for what we sought to achieve? *Did the activity need to be covert, or could the objectives have been achieved overtly?* *YOUR COMMENTS*	Yes	No

Was action taken to identify and minimise collateral intrusion? Did the applicant identify and describe possible collateral intrusion in all aspects of the operation? Did the applicant show that consideration has been given to removing/reducing likelihood of collateral intrusion? Could more have been done to limit/remove likelihood? *YOUR COMMENTS*	Yes	No

What evidence did applicant expect to gather? Did the applicant describe (a) what evidence he/she hoped to gain, and (b) the value of that evidence in relation to THIS enquiry? YOUR COMMENTS	Yes	No

Was the likelihood of obtaining confidential information considered?	Yes	No

If the application was for **CHIS** authorisation, were officers 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

Has the Authorising Officer considered the application appropriately and addressed the '5 Ws' and How? **Why** is the surveillance necessary? **Whom** is the surveillance directed against? **Where** will the surveillance take place? **When** will the surveillance take place? **What** surveillance activity / equipment was authorised? **How** are the surveillance objectives to be achieved?	Yes	No

Case Management – Reviews, Renewals and Cancellations	Yes	No
Have **reviews** been carried out in accordance with the authorisation?		
Are all **reviews** documented appropriately on the correct form and authorised? Is each review adequately supported by a summary of the operation to date, the information obtained so far, the reasons the surveillance should continue, and how the proposed activity is still		

proportionate to what it seeks to achieve?		
Are all **renewals** documented appropriately on the correct form and authorised?		
Are all **renewals** adequately supported by a summary of any significant changes to the original authorisation? Does the renewal set out the reasons it is necessary to continue with the surveillance, and why it is still proportionate to what it seeks to achieve? Are the reviews of the operation detailed in the renewal taking place, and outcomes noted?		
If the surveillance has concluded, has the appropriate **cancellation** been completed and authorised?		

Remember to submit a copy of this completed form to the Senior Responsible Officer (Head of Legal Services).