East Cambridgeshire District Council

**Appendix 2**

# OPERATIONAL POLICY AND GUIDANCE ON THE USE AND CONDUCT OF COVERT HUMAN INTELLIGENCE SOURCES AND AUTHORISATION UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000

**OPERATIONAL POLICY AND GUIDANCE ON THE USE AND CONDUCT OF COVERT HUMAN INTELLIGENCE SOURCES AND AUTHORISATION UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000, as amended (RIPA)**

## 1. What is a covert human intelligence source?

RIPA defines a Covert Human Intelligence Source (CHIS) as a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that

- Covertly uses such a relationship to obtain information or to provide access to information to another person; or
- Covertly discloses information obtained by the use of such a relationship, or because of the existence of such a relationship.

*RIPA does not apply to members of the public who volunteer information as part of their civic duties, or members of staff who report information in accordance with their contract of employment, or under the Council's Whistleblowing Policy.*

## 2. When is a relationship covert?

A relationship is covert if it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

## 2A. Internet and Social Networking Sites

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

An authorisation for the use and conduct of a CHIS may be needed if a relationship is established or maintained by the officer on behalf of the Council without disclosing his or her identity (i.e., the activity will be more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a social networking site.

An Officer must not set up a false identity for a covert purpose without authorisation.

An officer should not adopt the identity of a person known, or likely to be known, to the subject of interests or users of the site without authorisation, and without the explicit consent of the person whose identity is used, and without considering the protection of that person.

## 3. When might the Council use human intelligence sources?

The Council is involved in every day functions of law enforcement, which are mainly carried out in an overt manner. However, there will be occasions when

Council officers undertake their duties in a covert manner, for example, Trading Standards might use an informer (CHIS) as part of their enforcement function. The use of CHIS is only undertaken for serious issues and where there is a pressing need for the Council to act to protect the local community. All officers involved in activities affected by this Policy must observe the guidance contained in this document.

RIPA provides a framework for regulating the use of those investigatory powers. The Act ensures that any law enforcement activities that involve the use of a CHIS are consistent with the duties imposed upon public authorities by the Human Rights Act. RIPA provides that the use and conduct of a CHIS will be lawful if an authorisation has been lawfully issued and a person acts in accordance with that authorisation. This is important because if the Council is involved in any proceedings before a Court the Council will be able to show that it has acted lawfully and that it has gathered evidence properly.

The Council has to be satisfied that:

- *Any use and conduct of a CHIS are undertaken in connection with a statutory function with which the Council is charged.*

- *That such interference can be justified legally.*

- *The use and conduct of a CHIS are properly authorised in accordance with this Policy and consequently provides a basis for justifying any interference with a person's human rights.*

## 4. Authorising the use and conduct of a covert human intelligence source

If the use and conduct of a CHIS is being considered, urgent legal advice should be sought from the Director Legal and Monitoring Officer or Legal Services before any application for authorisation is submitted.

An application for authorisation should be submitted to an Authorising Officer. If approved, it will then need to be submitted to a Justice of the Peace for judicial approval.

The Act, as amended, identifies Authorising Officers as Director, Head of Service, Service Manager or equivalent. In East Cambridgeshire, this will be construed as a member of the Corporate Management Team, the Chief Executive and Service Leads.

Ideally the Authorising Officer should not be responsible for authorising a CHIS within their own direct sphere of activity, i.e., those operations or investigations in which they are directly involved or for which they have direct responsibility, or in which they would be the Controller.

The Protection of Freedoms Act 2012 amended RIPA to make local authority authorisation of a CHIS subject to judicial approval by a Justice of the Peace.

***Throughout this Policy and Guidance, the term 'authorisation' refers to an Authorisation granted by an Authorising Officer. Such an Authorisation once granted requires judicial approval before it becomes effective. In this Policy and Guidance, the term 'approval' refers to that judicial approval.***

**5. How is an application for authorisation made?**

An application for authorisation for the use or conduct of CHIS must be in writing and use the application form held on the central U drive. It should specify:

- The reasons why the authorisation is necessary in the particular case for the prevention or detection of crime or prevention of disorder.
- Details of the purpose for which the CHIS will be tasked or deployed.
- An account of the investigation or authorisation.
- The identities, where known, of those who are to be the subject of the use or conduct of the CHIS.
- Details of what the CHIS will be asked to do.
- The potential for collateral intrusion, that is to say, interference with the privacy of persons other than the subjects of the investigation, and why the intrusion is justified.
- The likelihood of obtaining any confidential information, what that might be, and how that will be treated.
- The reasons why the proposed use and conduct of CHIS is considered proportionate to what it seeks to achieve.
- The level of authorisation required.

**6. What will the Authorising Officer have to consider before granting an authorisation?**

Authorising Officers, and officers authorised to handle and/or control a CHIS, must be familiar with the requirements of the statutory Codes of Practice issued by the Home Office.

An authorisation can only be granted if the proposed covert activity aims to prevent or detect crime or prevent disorder. The proposed activity should relate to a specific purpose that is part of the Council's statutory or core functions. The concept of statutory or core functions of public authorities is not expressly mentioned as such in RIPA. It is not easy to define the concept in general terms or to propound a general test for distinguishing between the core functions and the ordinary functions of public authorities. However, such a distinction is implicitly recognised in RIPA by the nature of the grounds on which the Council may be authorised to use CHIS under RIPA, that is, to prevent or detect crime or to prevent disorder.

To grant an authorisation, the Authorising Officer must be satisfied that the authorisation is ***necessary*** for the purpose of preventing and detecting crime or preventing disorder.

The Authorising Officer must also believe that the use of CHIS is ***proportionate*** to what it seeks to achieve and ensure that satisfactory arrangements exist for the management of the CHIS. The Authorising Officer must believe that any potential for ***collateral intrusion*** and the likelihood of acquiring any ***confidential material*** is reduced to a minimum.

There must be adequate arrangements for maintaining the records of the exercise and controls in place to deal with any ***confidential material*** acquired.

There must be a record of whether authorisation was given or refused, by whom, and the time and date (see central U drive). In urgent cases where oral authorisation was initially given the written form should record the reasons for this.

The Authorising Officer must put in place a schedule of review dates for any CHIS authorisation.

*N.B. The safety of the public and Council staff must override all other considerations. Authorising Officers must consider violence at work, fatigue, lone working, etc. Where appropriate the Authorising Officer should call for a risk assessment to be conducted before granting the authorisation.*

## 7. What does the term "necessary" mean?

RIPA provides a framework for ensuring that any surveillance activities do not infringe the human rights of the individual. In considering whether to grant an authorisation, the Authorising Officer must consider whether the proposed conduct is ***necessary***.

The fact that a crime may have been, or is about to be committed, does not automatically mean that the use of a CHIS is necessary. There must be a pressing need for a covert operation to be undertaken and there must be a clear reason for the covert activity. Council Officers should not seek to obtain information through covert means that is not needed for an investigation. It might be useful and very interesting to acquire information about a particular individual, but if it is not strictly necessary to have it then officers should not seek to obtain it. Officers need to show why it is necessary in this case and at this time.

## 8. What does the term "proportionate" mean?

Proportionality is a very important concept. At its simplest, proportionality is about balancing the human rights of the individual against the operational need for the use of CHIS to further an investigation. An authorisation should not be granted upon grounds of the seriousness of the offence alone.

Any interference with a person's rights must be appropriate and justifiable. An Authorising Officer must consider a number of issues in deciding if a proposed course of action is proportionate. Most important is the belief that the Council

has relevant and sufficient reason for interfering with an individual's right to respect for family and private life.

If an Authorising Officer decides that the required information needs to be acquired through the use of a CHIS and that it cannot reasonably be acquired by other means that would involve less, or no, invasion of privacy that decision must be carefully documented and show how the Council has:

- Balanced the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm.

- Explained how and why the methods to be adopted will cause the least possible intrusion on the subject and others.

- Determined whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation.

- Evidenced, as far as reasonably practicable, what other methods had been considered and why they were not implemented or have been implemented unsuccessfully.

- Considered whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought.

Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances. Thus, where surveillance is proposed the covert action must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary; and the impact on the individual or group of people concerned must not be too severe.

Every case must be considered on its merits. What is proportionate in some circumstances will not be proportionate in others. Authorising Officers need to ensure that an applicant has considered other ways to obtain the required information, or evidence, such as use of third-party information powers and other sources.

**9. What does the term "collateral intrusion" mean?**

Collateral intrusion occurs when the use of CHIS interferes with the private and family life of people unconnected with the investigation. Authorising Officers must consider the likelihood and extent of collateral intrusion when considering any application and ensure that applicants have planned to minimise collateral intrusion. Situations where collateral intrusion can occur include where:

- Observing business premises may result in watching unconnected people come and go.

- During an operation observing or overhearing other conversations that are not relevant to the investigation and impact upon the privacy of others.

**10. What does the term "confidential material" mean?**

Confidential material is anything

- Which is subject to legal privilege, for example communications between a legal adviser and his/her client.
- Which is confidential personal information, for example information about a person's health or spiritual counselling or other assistance given or to be given to him or her.
- Which is confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and subject to an undertaking to hold in confidence.

**11. Are there any special rules for confidential material?**

The following requirements apply where the use or conduct of CHIS may result in acquiring knowledge of confidential material:

- The Authorising Officer must be the Chief Executive, or in his absence the person acting as Head of Paid Service.
- The application for authorisation must include an assessment of how likely it is that confidential material will be acquired.
- In the case of legally privileged material, an additional approval may be required from a Judicial Commissioner and reference should be made to the Home Office Code of Practice.
- Those involved in the operation must be advised that confidential material may be involved.
- Confidential material should not be retained or copied unless there is a clear relevant and specific purpose and should be destroyed when no longer needed.
- Confidential material should only be disclosed to those who have a clear and substantial need to know and for a specific and proper purpose.
- Confidential material must be clearly marked or accompanied by a clear warning of its confidentiality.

## 12. Can a child be a Covert Human Intelligence Source?

For the purposes of this policy, a child is a defined as a person under the age of 18. Special safeguards apply where the CHIS would be a child. Authorisation should not be granted unless:

- A risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the child.

- The risk assessment has been considered by the Authorising Officer and they are satisfied that any risks identified in it have been properly explained; and

- The Authorising Officer has given particular consideration as to whether the child is to be asked to get information from a relative, guardian, or any other person who has for the time being taken responsibility for the welfare of the child. A child under the age of 16 must never be asked to give information against their parents or any person who has parental responsibility for them.

  Authorisation should not be granted unless the Authorising Officer believes that management arrangements exist which will ensure that there will be at all times a person who has responsibility for ensuring that an appropriate adult will be present at any meetings between Council representatives and a CHIS under 16 years of age.

  Authorisations for the use of a child as a CHIS can be granted only by the Chief Executive or in his absence by the person acting as Head of Paid Service.

## 13. Can vulnerable persons act as a Covert Human Intelligence Source?

Only in the most exceptional circumstances should a vulnerable person be authorised to act as a CHIS and the authorisation must be given by the Chief Executive or in his absence by the person acting as Head of Paid Service.

## 14. Applying for judicial approval

Following the issue of an authorisation by an Authorising Officer, the applicant should contact Legal Services so that a hearing may be arranged at the Magistrates Court to approve the grant of the authorisation. The applicant should be aware of the process for obtaining prompt or out-of-hours judicial approval if required. All relevant paperwork should be available for the Court to examine and officers should complete the judicial approval form on the central U drive. A Justice of the Peace will make one of the following decisions:

- **Approve the application**

  If the application is approved the Justice of the Peace will make an order and the Council is now able to use the CHIS for that particular case.

- **Refuse to approve the application**

  The RIPA authorisation will not take effect and the Council cannot use the CHIS in that case.

  If an application has been refused the Council may wish to consider the reasons for that refusal, for example, a technical error in the form may be remedied without going through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken.

- **Refuse to approve the grant and quash the authorisation**

  This applies where a Justice of the Peace refuses to approve the grant and additionally decides to quash the authorisation. The Court must not exercise its power to quash the authorisation unless the applicant has had at least two business days from the date of the refusal in which to make representations.

**15. What management arrangements should be in place for the Covert Human Intelligence Source?**

The following persons must be nominated in relation to each CHIS:

| | |
|---|---|
| A Handler | this person must be an officer of the Council and that person will have day-to-day responsibility for dealing with the CHIS and for the CHIS's security and welfare. The Handler will need to explain to the CHIS what they must do, for example, a CHIS may be someone who assists a trading standards officer who is asked to undertake a test purchase of items that have been labelled misleadingly. |
| A Controller | this person must be an officer of the Council and that person will have a general oversight of the use made of the CHIS. |
| A Record Keeper | this person must be an officer of the Council who is given the responsibility for maintaining the records relating to the CHIS and the use of the CHIS. |

It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the Handler asks the CHIS to do something. Rather, an authorisation might cover, in broad terms, the nature of the CHIS's task. If the nature of the task changes significantly, then a fresh authorisation

may need to be sought. When unforeseen action occurs, it must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient, a new authorisation should be obtained before any further such action is carried out.

The day-to-day contact with the CHIS is to be conducted by the Handler. Some arrangements may be made in direct response to information provided by the CHIS on their meeting with the Handler. Steps should be taken to protect the safety and welfare of the CHIS when carrying out actions in relation to an authorisation and of others who may be affected by the actions of the CHIS.

Before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any action and the likely consequences should the role of the CHIS become known to the subject of the investigation or those involved in the activity which is being investigated. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

The Handler is responsible for bringing to the Controller's attention any concerns about the personal circumstances of the source, insofar as they might affect:

- The validity of the risk assessment
- The conduct of the CHIS, and
- The safety and welfare of the CHIS.

Where deemed appropriate, the Controller must ensure that the information is considered by the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

Officers tasked with carrying out duties associated with the use and conduct of a CHIS must see a copy of the Authorisation and any comments by the Authorising Officer. In particular, the Handler should not proceed until the Authorisation has been seen. There should be an acknowledgement in writing (with date and time) that the Authorisation has been seen.

.

**16. What type of things can a CHIS be asked to do?**

Once authorised a CHIS could be asked to obtain information, to provide access to information, or to act otherwise or act incidentally for the benefit of the Council in the performance of its statutory enforcement and regulatory functions. The CHIS might be asked to wear or carry a surveillance device. No additional authorisation is required if the CHIS is invited into a private vehicle or residential premises. A CHIS must not be asked to install a surveillance device nor intercept post or any other communications including those sent by telephone or e-mail.

A CHIS must not be asked to do anything or not to do something that would involve the commission of a criminal offence by the CHIS, for example, a CHIS must not be asked to steal a document to get information.

**17. How long will an authorisation last?**

An authorisation will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of a juvenile CHIS. In the case of a juvenile CHIS, authorisation will cease at the end of a period of 4 months beginning with the date on which it took effect.

**18. Reviewing authorisations**

It is the duty of Authorising Officers to undertake regular reviews of authorisations to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include the use made of the CHIS during the period authorised; the tasks given to the CHIS; the information obtained from the CHIS; and the reasons why executive action is not possible at this stage. Reviews should be more frequent where the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

Reviews must be recorded using the relevant review form on the central U drive.

If a decision is taken to cease using a CHIS, an instruction must be given to those involved in the operation to stop using the CHIS as an information source. The date on which that instruction is given should also be recorded.

N.B. A Justice of the Peace does not consider internal reviews.

**19. Renewing authorisations**

If an applicant wishes to continue the use of a CHIS for the same purpose for which authorisation was given, then he/she may apply to renew it in writing for a further period of 12 months beginning with the day when the authorisation would have expired but for the renewal.

Any request for a renewal of an authorisation should be recorded using the Renewal Form on the central U drive outlining the following:

- Whether this is the first renewal, or on how many occasions it has been renewed.
- Details of any significant changes to the information given in the previous or original authorisation.
- The reasons why it is necessary to continue to use the CHIS.
- The use that has been made of the CHIS since the Authorisation/last renewal; the tasks given to the CHIS during that period; and the information obtained by the CHIS.

- The results of the reviews of the use of the CHIS.
- An estimate of the length of time the CHIS will continue to be operational.

Any renewal will follow a similar process to an Authorisation for judicial approval by a Justice of the Peace (see paragraph 14 above).

**20. Cancelling an authorisation**

The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the use or conduct of the CHIS no longer meet the criteria for authorisation. If that Authorising Officer is unavailable, another Authorising Officer must undertake that role and ensure that use of the CHIS ceases. Cancellation must be recorded using the relevant cancellation form on the central U drive.

N.B. A Justice of the Peace does not consider cancellations.

Where necessary, the safety and welfare of the CHIS should continue to be considered after the authorisation has been cancelled. The Authorising Officer will wish to satisfy themselves that all welfare matters are addressed.

**21. What records must be kept?**

The following records must be maintained by the Record Keeper in a manner that will preserve the identity of the source and the information which they supply. It is important to note that RIPA requires that documents which contain the true identity of the CHIS should be kept secure and separately from other documents and only those with a need to know the true identity of the CHIS should be able to access them.

- Full details of the CHIS and the management arrangements. This will include:

- *The identity of the CHIS*

- *The identity or identities used by the CHIS, where known*

- *The means used within the Council of referring to the CHIS*

- *Any significant information connected with the security and welfare of the CHIS*

- *Any confirmation made by an Authorising Officer granting or renewing an authorisation for the conduct or use of a source, that the security and welfare of the CHIS has been considered and that any identified risks to the security and welfare of the CHIS have been properly explained to and understood by the CHIS*

- *The date when, and the circumstances in which, the CHIS was recruited*

- *The authority for the related investigation or operation*
- *The identities of the Controller, the Handler, and the Record Keeper*
- *The period for which those responsibilities have been discharged by those persons*
- *The tasks that are given to the CHIS and the demands made of him in relation to his activities as a CHIS*
- *All contacts or communications between the CHIS and the Council or where the CHIS is a Council Officer, the Handler, and the Controller.*
- *The information obtained by the Council by the conduct or use of the CHIS*
- *In the case of a CHIS who is not an Officer of the Council, every payment, benefit or reward or every offer of a payment, benefit or reward that is made or provided by or on behalf of the Council in respect of the CHIS's activities for the benefit of the Council*

- A copy of the application for authorisation.
- A copy of the authorisation.
- A copy of the application for judicial approval.
- A copy of the judicial approval.
- Any risk assessment made in relation to the CHIS.
- The circumstances in which tasks were given to the CHIS.
- The value of the CHIS to the Council.
- A record of the period over which the surveillance is taking or has taken place (including any significant suspensions of use of the CHIS).
- A record of the result of any periodic reviews of the authorisation.
- A copy of any renewal of authorisation, together with the supporting documentation submitted when the renewal was requested.
- A copy of the cancellation of the authorisation.

These records should be retained for a period of at least five years.

**22. Who may see the records?**

Only those people who need to know, otherwise they are strictly confidential.

**23. The Central Record**

The Director Legal and Monitoring Officer will maintain a Central Register of authorisations. The Central Register needs only to contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed, or cancelled, and an indication as to whether the activities were self-authorised.

The Central Register will be held electronically and access restricted.

Authorising Officers are responsible for ensuring that they provide timely information to enable the central register to reflect all current activities and to avoid duplication of resources.

**24. Who is responsible for overseeing compliance with RIPA?**

Under the Investigatory Powers Act 2016, the Investigatory Powers Commissioner has been appointed to provide independent oversight of the use of the powers contained in Part 2 of the Act. Inspectors from the Investigatory Powers Commissioner's Office will inspect the Council from time to time to ensure that the Council is complying with the Act.

In addition, the Act establishes an Independent Tribunal. This Tribunal has full powers to investigate and decide any case where a person complains about the conduct of the Council in exercising its powers of carrying out surveillance.

This Policy also forms part of the Councils quality protocols and as such is liable to scrutiny. All officers involved in activities affected by this Policy must observe the guidance contained in this document.

**25. What reference documents are there?**

The Council and those persons acting under Part 2 of the Act must have regard to the Codes of Practice issued under the Act. Each Authorising Officer will have copies of these Codes. In addition, the Council has prepared seven specific forms for use by officers in relation to CHIS. These forms are available on the central U drive.

Where fraud or corruption is suspected, then regard should be had to the Council's Anti-Fraud and Corruption Strategy.

**26, Training**

26.1 Appropriate corporate training will be arranged by the Director Legal & Monitoring Officer for all officers likely to make applications or authorise them.

26.2 The Director Legal & Monitoring Officer will ensure suitable training is in place for all new members of staff who undertake an enforcement role. This may be conducted by way of a briefing, an e-learning module or with an external trainer. Service Leads of enforcement teams must ensure new staff undertake RIPA training within six months of their start date.

26.3 Authorising Officers must receive training on an annual basis, which may be conducted by way of a briefing, an e-learning module or with an external trainer.

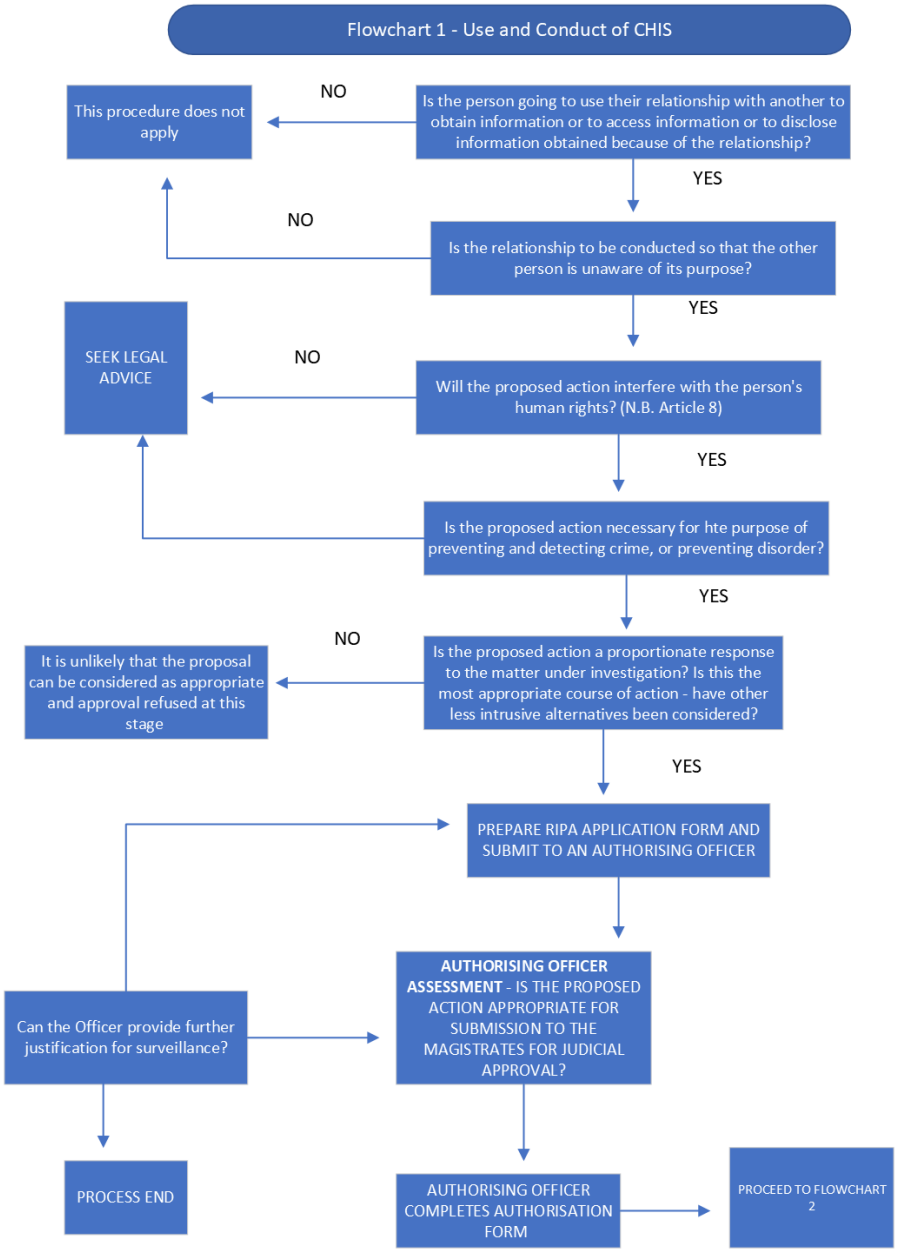
26.4 All other identified staff will be required to attend annual refresher training, either by way of a briefing, an e-learning module or with an external trainer. It

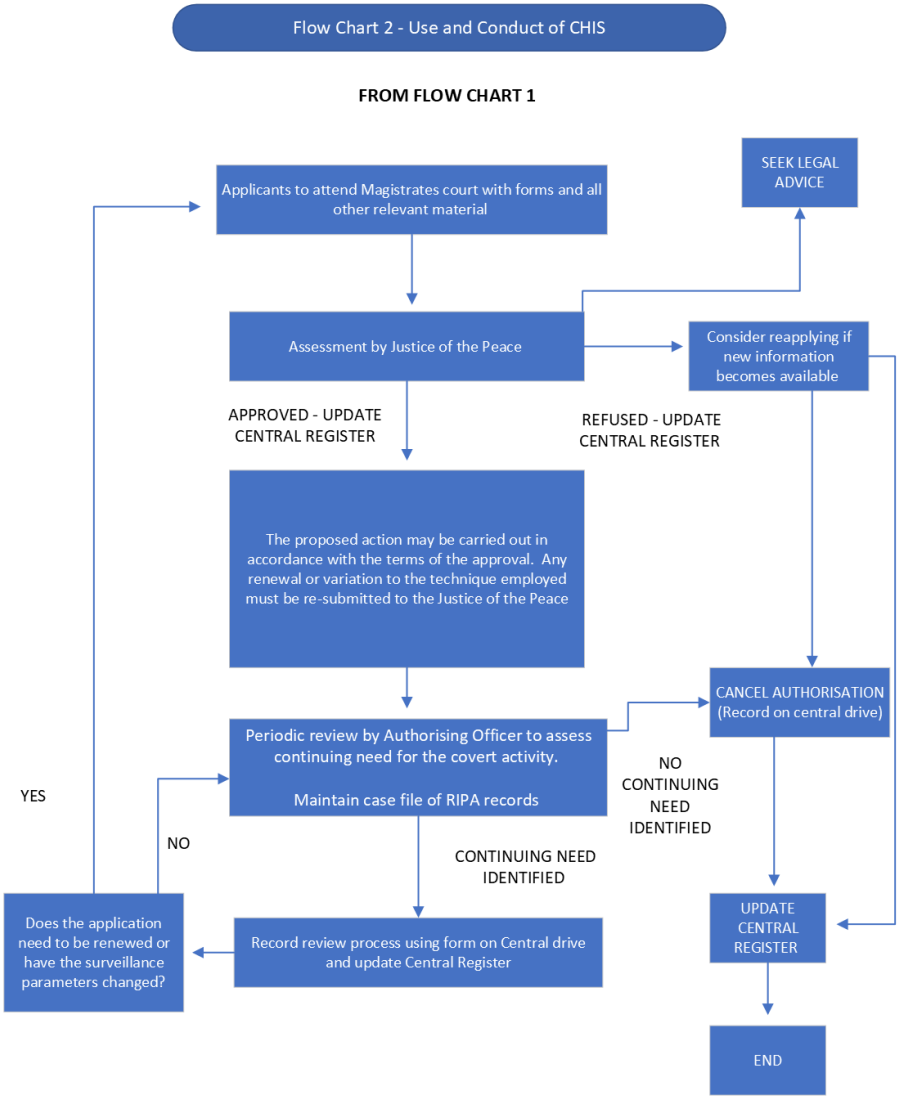
is the responsibility of Service Leads of enforcement teams to ensure relevant staff are identified and receive such training.

26.5 Officers may in any event supplement corporate training by attending appropriate external training courses and seminars and will notify the Director Legal & Monitoring Officer of any additional training undertaken, which will be noted.

26.6 No officer will be permitted to make applications or undertake the role of an Authorising Officer unless they have undergone suitable training approved by the Director Legal & Monitoring Officer.

**Formatted:** Indent: Hanging: 1.27 cm


Flowchart 1 - Use and Conduct of CHIS
Is the person going to use their relationship with another to obtain information or to access information or to disclose information obtained because of the relationship?
NO
This procedure does not apply
YES
Is the relationship to be conducted so that the other person is unaware of its purpose?
NO
YES
Will the proposed action interfere with the person's human rights? (N.B. Article 8)
NO
SEEK LEGAL ADVICE
YES
Is the proposed action necessary for hte purpose of preventing and detecting crime, or preventing disorder?
YES
Is the proposed action a proportionate response to the matter under investigation? Is this the most appropriate course of action - have other less intrusive alternatives been considered?
NO
It is unlikely that the proposal can be considered as appropriate and approval refused at this stage
YES
PREPARE RIPA APPLICATION FORM AND SUBMIT TO AN AUTHORISING OFFICER
AUTHORISING OFFICER ASSESSMENT - IS THE PROPOSED ACTION APPROPRIATE FOR SUBMISSION TO THE MAGISTRATES FOR JUDICIAL APPROVAL?
Can the Officer provide further justification for surveillance?
PROCESS END
AUTHORISING OFFICER COMPLETES AUTHORISATION FORM
PROCEED TO FLOWCHART 2


Flow Chart 2 - Use and Conduct of CHIS
FROM FLOW CHART 1
Applicants to attend Magistrates court with forms and all other relevant material
SEEK LEGAL ADVICE
Assessment by Justice of the Peace
Consider reapplying if new information becomes available
APPROVED - UPDATE CENTRAL REGISTER
REFUSED - UPDATE CENTRAL REGISTER
The proposed action may be carried out in accordance with the terms of the approval. Any renewal or variation to the technique employed must be re-submitted to the Justice of the Peace
CANCEL AUTHORISATION (Record on central drive)
Periodic review by Authorising Officer to assess continuing need for the covert activity.
Maintain case file of RIPA records
NO CONTINUING NEED IDENTIFIED
YES
NO
CONTINUING NEED IDENTIFIED
Does the application need to be renewed or have the surveillance parameters changed?
Record review process using form on Central drive and update Central Register
UPDATE CENTRAL REGISTER
END