**East Devon District Council**

**Policy on use of directed surveillance and covert human intelligence sources - Regulation of Investigatory Powers Act 2000**

**Reviewed**
March 2021

**Policy Approval**
Audit and Governance Committee on 20th January 2022.

**Reasons for introducing the Policy**
To explain legal requirements and act as a brief guide to the legislation for Council staff.

**Policy Statement**
The purpose of this procedure is to ensure that the Council complies with the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA') and that appropriate authorisations are given for directed surveillance and the use of covert human intelligence sources ('CHIS').

RIPA, together with its associated regulatory framework, provides a valuable protection to the Council if directed or covert surveillance is carried out, and may protect the Council from the risks of civil action in the event of a breach of a person's human rights. In addition, its correct application may ensure that evidence gained by such means will be admitted in evidence more readily in the criminal courts.

The policy sets out the tests which must be applied in deciding whether authorisation is appropriate. RIPA now restricts directed surveillance to serious criminal cases or to tobacco or licensing offences related to children. Authorisations for directed surveillance or covert human intelligence sources are not effective until approved by a Justice of the Peace (Magistrate).

**Terms Explained**
These are set out in the policy at appropriate points in the context of the legislation.

**How will we go about it?**
The policy has been approved by members, and senior and relevant staff have been trained on its implementation and will be provided with regular refresher training.

**Specific Policy Areas**

## 1 INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 controls the use of covert investigative techniques by public authorities. It provides for the application for and granting of authorisations for those techniques covered by the Act.

1.2 Article 8 of the European Convention on Human Rights which has been incorporated into UK legislation provides a right to private and family life. This

is not an absolute right; it may be infringed in certain circumstances. The RIPA is designed to provide a statutory regulatory framework, which will meet the requirements of the European Convention on Human Rights and the subsequent provisions in UK legislation.

## 2 ASSOCIATED DOCUMENTS

### 2.1 Relevant Statutes

(a) Regulation of Investigatory Powers Act 2000 as amended by the Protection of Freedoms Act 2012 and explanatory notes
(b) Investigatory Powers Act 2016
(c) Human Rights Act 1998
(d) Police and Criminal Evidence Act 1984

**Relevant Statutory Instruments (include)**

(e) Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 (SI 2003 No 3171) as amended by Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010/521 as amended and Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012/1500
(f) The Regulation of Investigatory Powers (Juveniles) Order 2000/2793
(g) The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

### 2.2 Relevant Guidance

(a) Protection of Freedoms Act 2012 – Home Office Guidance
(b) Code of Practice for covert surveillance and property interference
(c) Code of Practice for covert human intelligence sources
(c) Codes of Practice for the acquisition and disclosure of communications data and retention of communications data
(d) Code of Practice for investigation of protected electronic information
(e) Guidance from Investigatory Powers Commissioner's Office – website
(f) Guidance from the Home Office on the judicial approval process for RIPA and crime threshold for directed surveillance

All RIPA Codes, relevant legislation and guidance can be found on the Government website. Further guidance and advice is also available on the Investigatory Powers Commissioner's Officer (IPCO) website. IPCO independently oversee the use of investigatory powers, ensuring they are used in accordance with the law and in the public interest. In a case where it is felt that requirements have not been followed, the non-compliance can be reported as an 'error' and IPCO will, in the case of a serious matter, investigate the matter further.

## 3 SCOPE

The Act provides a regime of primary legislation and Codes of Practice, which divide covert investigation techniques into categories distinguished to an extent by the degree of intrusion involved. This procedure applies to all investigation and surveillance that may be subject of an authorisation under RIPA.

3.1 The Act provides the following investigatory powers:

(1) Part 1(Chapter I) – interception of communications
(2) Part 1 (Chapter II) – the acquisition of communications related data e.g. telephone billing data
(3) Part II deals with:
- intrusive surveillance on residential premises or in private vehicles
- directed surveillance, that is covert surveillance in the course of a specific operation
- the use of covert human intelligence sources e.g. agents, informants, undercover officers

(4) Part III – deals with the power to seize electronic keys giving access to encrypted computer material
(5) Part IV – provides for scrutiny, complaint procedures and codes of practice.

3.2 This policy document relates to the **use of directed surveillance** and **covert human intelligence sources**.

3.3 RIPA sets out the purposes for which each of these powers may be used, the Agencies and authorities that can use them and who should authorise the use. Authorisation under RIPA gives lawful authority for the use of these methods of obtaining information provided there is compliance with the statutory requirements and procedures. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenge under the Human Rights Act 1998.

3.4 Services likely to conduct investigations covered by RIPA are Planning, Environmental Health, Housing, Licensing and Revenues & Benefits. **However, before conducting an investigation using methods or techniques covered by this Act, the officer doing so is required to seek the necessary authorisations.**

3.5 Care must be taken that covert surveillance does not become intrusive surveillance. Intrusive surveillance is **only** available to the Home Office, MI5 and certain other central government bodies, **not to councils**.

3.6 Intrusive surveillance is defined in Section 26(3) of RIPA which states that it is intrusive surveillance only if it is covert and it;
- is carried out in relation to anything taking place on residential premises or in a private vehicle; and

- involves the presence of an individual on the premises or vehicle or is carried out by a surveillance device.

## 4 ACTIVITY REQUIRING AUTHORISATION

4.1 The following types of activity will require authorisation:
- directed surveillance
- the conduct and use of covert human intelligence sources

4.2 Directed surveillance is, in essence, any activity undertaken covertly for the purpose of a specific investigation in such a way that is likely to result in obtaining information about a person's private life.

4.3 A covert human intelligence source (CHIS) is usually, but not always an inside informant or undercover officer who develops or maintains their relationship with the surveillance target, having the covert purposes of obtaining or accessing information for the investigator. Under the 2000 Act, a person is a CHIS if:

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

## 5 APPLYING FOR AUTHORISATIONS

5.1 The authorising officers for the Council are; the Chief Executive (Mark Williams), s.151 Finance Officer (Simon Davey) and Monitoring Officer and RIPA Senior Responsible Officer (Henry Gordon Lennox).

5.2 Any officer intending to use directed surveillance or a CHIS shall apply for authorisation by completing the appropriate application form - **DS/1 -** Application for the use of Directed Surveillance **or CHIS/1-** Application for the use of Covert Human Intelligence Sources (CHIS) - and consult with the RIPA Co-ordinating Officer, who is the Principal Solicitor and Deputy Monitoring Officer (Anita Williams) who is also the central point for advice on law and procedure. She will submit completed authorisations to an authorising officer for consideration and advise the officer of the decision. In line with government guidance, the investigating officer will be responsible for making the application to the Magistrates' Court and attending any hearing.

5.3 **Confidential information and vulnerable or juvenile CHISs**
Where the likely consequence of the directed surveillance or conduct of a source would be for any person to acquire knowledge of confidential information, the deployment of a source must be subject to special authorisation. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. The use of vulnerable or juvenile CHISs requires special authorisation and there

is a shorter authorisation period for juvenile CHISs. In these cases the proposed course of conduct must be referred to the Chief Executive, or in his or her absence to the person acting as Head of Paid Service, for a decision as to whether authorisation may be granted. See Code of Practice for covert surveillance and property interference, Section 4 and Annex A

5.4 Broadly speaking, legal privilege extends to communications between lawyers and their clients, but not where that communication has a criminal purpose.

5.5 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

5.6 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, information from a patient's medical records or information held by a stockbroker which has been acquired or created in the course of the profession or business, including communications in which personal information is acquired or created.

5.8 In those cases where confidential information has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested. Any application for authorisation to acquire confidential data should only be made where there has been prior consultation with the RIPA Co-ordinating Officer or other qualified legal officer.

## 6 GRANTING OF AUTHORISATIONS FOR DIRECTED SURVEILLANCE

6.1 Section 28 provides that a person shall not grant authorisation for *directed surveillance* unless he believes that:

6.1.1 the authorisation is **necessary** in the circumstances for the purpose of;

- preventing or detecting conduct which is a criminal offence being an offence punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment, or
- offences relating to the underage sale of alcohol and tobacco (*being those offences listed in Article 7A of the 2010 Order [SI: 2010/521] as amended*), or
- preventing disorder where such disorder involves a criminal offence punishable (whether on summary conviction or indictment) by a maximum term of 6 months' imprisonment,

and therefore any application must address **why** it is necessary.

6.1.2 the authorised surveillance is **proportionate** to what is sought to be achieved by it. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6.2 A local authority may **not** authorise the use of directed surveillance under RIPA to investigate conduct or disorder that does not involve criminal offences or to investigate low level offences which may include, for example, littering, dog control and fly-posting. At the start of an investigation, council officers will need to satisfy themselves they are investigating a criminal offence punishable by a prison term of 6 months at least (unless related to under age tobacco and alcohol sales).

6.3 The authorising officer in determining whether the surveillance is proportionate will give particular consideration to any collateral intrusion on or interference with the privacy of persons other than the subject(s) of the surveillance. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

6.4 The Council officer must obtain an authorisations in writing from an authorising officer (see Section 5). Wherever possible authorising officers should not be responsible for authorising the activities of their own services.

6.5 Having obtained a written authorisation, it is then necessary to obtain the approval of a Justice of the Peace (Magistrate) ('JP'). The Home Office has issued guidance (which can be found here) on the judicial approval process as well as the relevant forms to use.

6.6 The RIPA Co-ordinating Officer (Deputy Monitoring Officer) will organise for the completion of the judicial application / order form with the investigating officer and liaise with Her Majesty's Court Service to arrange a hearing.

6.7 The investigating officer and authorising officer will attend the Court hearing with the application ready to answer the JP's questions, although the forms and supporting papers must by themselves make the case.

6.8 If the JP is satisfied that the statutory tests have been met and continue to be met and that the use of the technique is necessary and proportionate s/he will issue an order approving the grant or renewal. The JP will also check that the Council authorising officer was an appropriate designated person within the council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met. This assessment does not remove or reduce in any way the

duty of the Council's authorising officer to determine whether the tests of necessity and proportionality have been met.

6.9 The application/order signed by the JP and the original RIPA authorisation will need to be retained by the Council and kept on the central register maintained by the RIPA Co-ordinating Officer.

6.10 The 2012 Home Office Guidance states that in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. Therefore local councils may need to work with the police if faced with an emergency.

6.11 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).

6.12 **Duration of Directed Surveillance Authorisations and Reviews**
An authorisation in writing ceases to have effect at the end of a period of 3 months beginning with the day on which it took effect, being the date of authorisation by the JP. So an authorisation starting 1 January would come to an end on 31 March. Regular reviews of authorisations should be undertaken. If, during an investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold (of at least a maximum of 6 months in prison) the use of directed surveillance should cease. The results of the review should be recorded on **DS/2** Review of the use of directed surveillance and a copy filed on the central record of authorisations. If the surveillance provides access to confidential information or involves collateral intrusion more frequent reviews will be required. The authorising officer should determine how often a review should take place.

6.13 **Renewals**

6.13.1 While an authorisation is still effective the authorising officer can renew it if he considers this necessary for the purpose for which the authorisation was originally given. The authorisation will be renewed in writing for a further period, beginning with the day when the authorisation would have expired, but for the renewal, and can be for a further period of 3 months.

6.13.2 Applications requesting renewal of an authorisation are to be made on the appropriate form as set out at **DS/3** Renewal of directed surveillance and be submitted to the authorising officer.

6.13.3 Applications for renewal will record:

- whether this is the first renewal, if not, the occasion which the authorisation has previously been renewed
- the information as required in the original application, as it applies at the time of the renewal; together with;
    - the significant changes to the information in the previous authorisation

- the reasons why it is necessary and proportionate to continue with the surveillance
- the content and value to the investigation or operation of the information so far obtained by the surveillance
- an estimate of the length of time the surveillance will continue to be necessary

**Renewals will also require the approval of a JP in the magistrates' court before they can take effect and investigating officers should bear in mind the relevant timescales when considering the need to renew an authorisation.**

6.14 **Cancellations**

The person who granted or last renewed the authorisation **MUST** cancel it if he is satisfied that the directed surveillance no longer meets the criteria for authorisation. Requests for cancellation will be made on the appropriate form as set out at **DS/4** Cancellation of the use of directed surveillance.
and submitted to the authorising officer for authorisation of the cancellation. No JP's involvement is required for cancellation. When cancelling an authorisation, the authorising officer should:

- record the date and times (if at all) that surveillance took place and when the order to cease the activity was made
- the reason for cancellation
- ensure that the surveillance equipment has been removed and returned
- provide directions for the management of the product
- ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.
- record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

6.15 **Use of CCTV systems**

6.15.1 General operation of overt CCTV equipment and the use of any information it has gathered in a reactive operation will not require a RIPA authorisation as it is not viewed as directed surveillance (see Code of Practice Covert Surveillance and Property Interference eg. paragraph 3.36 - 3.39 .Use as part of a proactive investigation (i.e. to track individuals) may well require authorisation.

6.15.2 The Council has regard to the Surveillance Camera Code of Practice regarding the use of CCTV and has a policy relevant to it which can be found [*link to be provided when CCTV policy adopted*].

## 7 GRANTING OF AUTHORISATION FOR THE CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

7.1 The same requirements of 'necessity' and 'proportionality' exist for the granting of CHIS authorisations as are set down for directed surveillance (see *sections 6.1.1. and 6.1.2* above) but the crime threshold (i.e. the availability of 6 month prison sentence) **does not** apply.

7.2 Additionally the authorising officer shall not grant an authorisation unless he/she believes that arrangements exist for a CHIS which satisfy the following requirements:

- there will at all times be an officer with day to day responsibility for dealing with the source and the source's welfare
- there will at all times be an officer who will have general oversight of the use made of the source
- there will at all times be an officer with responsibility for maintaining a record of the use made of the source
- those records will always contain particulars of all such matters as may be specified for this purpose by the Secretary of State
- records which disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available

7.3 Similarly before authorising use or conduct of the source, the authorising officer must be satisfied that the conduct/use is proportionate to what the use or conduct of the source seeks to achieve, taking into account the likely degree of intrusion into privacy of those potentially effected or the privacy of persons other than those who are directly the subjects of the operation or investigation. Alternative means of gathering the evidence should be considered, and reasons given why this has been rejected. Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation. Where there is intrusion upon a target this and any collateral intrusion should be kept to a minimum.

7.4 Particular care is required where people would expect a high degree of privacy or where, as a consequence of the authorisation confidential material is likely to be obtained. Where confidential material is likely to be acquired, or a juvenile or vulnerable CHIS is used, then approval must be obtained from the Chief Executive, or in his absence, the person acting as Head of Paid Service.

7.5 Consideration is also required to be given to any adverse impact on community confidence that may result from the use or conduct of a source or information obtained from that source.

7.6 Additionally, the authorising officer should make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation. This should include the risk to the source of any task and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset. A responsible officer should be identified within the service concerned who will have day to day responsibility for the control and direction

and activities of the source, recording the information supplied by the source; and monitoring the source's security and welfare.

7.7 Authorisation for the use of a CHIS must be given in writing. **Care must be taken to make sure that covert surveillance does not become intrusive surveillance** *(see section 3.6 above for what this is)***, as this authority is not permitted to carry out intrusive surveillance**. **Application must also be made to a JP for authorisation before covert surveillance is undertaken.**

7.8 Ideally the authorising officers should not be responsible for authorising their own activities, e.g. those in which they themselves are to act as a source or in tasking a source. However it is recognised that this will not always be possible especially in the case of small departments.

7.9 An application for authorisation for the use or conduct of a source will be made on the appropriate form as set out at **CHIS/1** Application for the use of Covert Human Intelligence Sources (CHIS) and must record:

- The source's pseudonym or ref number
- The details of the handler
- The details of the manager with general oversight
- The person responsible maintaining records under the RIPA (Source Records) Regulations 2000
- Operation name
- Job title of authorising officer
- Purpose of specific operation or investigation
- The purpose for which the source will be tasked or deployed
- Details of what the source would be tasked to do
- Why the conduct or use of the source is necessary for the purpose of preventing or detecting crime or preventing disorder
- Why the conduct or use of the source is proportionate to what it seeks to achieve
- Details of potential collateral intrusion and why the intrusion is unavoidable, precautions to minimise collateral intrusion and how any will be managed, and whether the evidence could be obtained by any other means
- Any particular sensitivities in the local community where the source is to be used, and whether similar activities are being undertaken by other public authorities that could impact on the deployment of the source
- A risk assessment of the risk to the source in carrying out the proposed conduct
- Details of any confidential material that might be obtained as a consequence of the authorisation and confidential information authorisation

The RIPA (Source Records) Regulations 2000 (SI 2000/2725) further require a record to be kept of

- the identity of the source;
- the identity, where known, used by the source;
- any relevant investigating authority other than the authority maintaining the records;
- the means by which the source is referred to within each relevant investigating authority;
- any other significant information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- the date when, and the circumstances in which, the source was recruited;
- the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of him in relation to his activities as a source;
- all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- the information obtained by each relevant investigating authority by the conduct or use of the source;
- any dissemination by that authority of information obtained in that way; and
- in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

7.10 **Duration of Authorisations**

A written authorisation, unless renewed, will cease to have effect at the end of a period of twelve months (four months in the case of a juvenile CHIS) beginning with the day on which it took effect, being the date of authorisation by the JP.

7.11 **Renewals**

Authorisations for the conduct and use of CHIS can be renewed, the same criteria applying as on first authorisation. Applications for renewal must be made on the appropriate form as set out at **CHIS/3** Renewal of authorisation to use Covert Human Intelligence Sources and submitted to the authorising officer. However, an application for renewal should not be made until shortly before the authorisation period is coming to an end.

7.12 An authorisation may be renewed more than once – provided it continues to meet the criteria for authorisation. **Renewals must also be approved by a JP before they can take effect.**

7.13 **Reviews**

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on **CHIS/2** Reviewing the use of Covert Human Intelligence Sources (CHIS) and a copy filed on the central record of authorisations. If the surveillance provides access to confidential information or involves collateral intrusion frequent reviews will be required. The authorising officer should determine how often a review should take place.

7.14 Before an authorising officer renews an authorisation he must be satisfied that a review has been carried out of:

- The use made of the source during the period authorised
- The tasks given to the source
- The information obtained from the use or conduct of the source

7.15 If the authorising officer is satisfied that the criteria necessary for the initial authorisation continue to be met, he may renew it in writing for a further period. **Renewals must also be approved by a JP before they can take effect.**

7.16 **Cancellations**

The officer who granted or renewed the authorisation **MUST** cancel it if he/she is satisfied that

- the use or conduct of the source no longer satisfies the criteria for authorisation, or
- that the arrangements for the source's case no longer exist

7.17 Requests for cancellation will be made on the appropriate form as set out at **CHIS/4** Cancellation of Covert Human Intelligence Sources (CHIS) and submitted to the authorising officer for authorisation of the cancellation. The cancellation process does not involve a JP.

7.18 **Management Responsibility**

The day to day contact between the Council and the source is to be conducted by the handler, who will usually be an officer below the rank of the authorising officer. No vulnerable person or young person under the age of 18 should be used as a source.

7.19 **Security and Welfare**
Account must be taken of the safety and welfare of the source. The authorising officer prior to granting authorisation should ensure that an assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the target know the role of the source.

7.20 **Special Rules**
The fullest consideration should be given in cases where, the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his/her home, or where there are special sensitivities.

## 8 MAINTENANCE OF RECORDS

8.1 The RIPA Co-ordinating Officer is responsible for keeping in a dedicated place;

- a record of all authorisations sought
- a record of authorisations granted and refused
- applications for the granting, renewing and cancellation of authorisations
- a record of all JP approvals and renewals

The records will be confidential and will be retained for a period of 5 years (for both CHIS and directed surveillance) from the ending of the authorisation. It is intended that the Central Record will be spreadsheet format and represent the requirements of the Code of Practice for Covert Surveillance and property Interference (Chapter 8) and the Code of Practice for CHIS

8.3 Authorising officers will ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

8.4 Where material is obtained by surveillance which is wholly unrelated to a criminal or other investigation or the person subject of the surveillance and no reason to believe it will be relevant to future civil or criminal proceedings it should be destroyed immediately. The decision to retain or destroy material will be taken by the relevant authorising officer.

## 9 USE OF SOCIAL MEDIA FOR GATHERING EVIDENCE TO ASSIST IN ENFORCEMENT ACTIVITIES

9.1 As explained in this policy, the Regulation of Investigatory Powers Act 2000 regulates the use of covert surveillance activities by Local Authorities. Special authorisation arrangements need to be put in place whenever the Council considers commencing a covert surveillance or obtaining information by the use of informants or officers acting in an undercover capacity.

9.2 This also includes the use of social media sites for gathering evidence to assist in enforcement activities, as set out below:

- officers must not create a false identity in order to 'befriend' individuals on social networks without authorisation under RIPA.

- officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute their investigation.

- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate.

- officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

9.3 Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case directed surveillance authorisation will be required. If it becomes necessary to breach the privacy controls and become, for example, a 'friend' on Facebook, with the investigating officer utilising a false account concealing his/her identity as a Council officer for the purposes of gleaning intelligence, this is a covert operation intended to obtain private information and should be authorised, at a minimum, as directed surveillance. If the investigator engages in any form of relationship with the account operator then s/he becomes a CHIS requiring authorisation as such and management by a controller and handler with a record being kept and a risk assessment created.

## 10 Data Protection

Information ("product") obtained through directed surveillance or CHIS activity which is personal data will be dealt with in accordance with the Council's Data Protection Policy, relevant privacy notices and Document Retention Schedule. These can all be accessed from the data protection pages of the Council's website.

## 11 AWARENESS OF THE CONTENTS OF THE ACT AND TRAINING

It shall be the responsibility of the RIPA Co-ordinating Officer to have oversight of the training programme (to be organised by the H.R. training team) and to ensure that all staff involved or likely to be involved in investigations or enforcement receive a copy of the training document, have received training and are aware of the requirements and implications of the Act.

## 12 CODES OF PRACTICE

A copy of each Code of Practice shall be kept in the reception area and be available to members of the public during usual working hours.

**Outcomes**
A clear policy should support a positive outcome when the Council is next inspected by the Office of the Surveillance Commissioner.

**Who is responsible for delivery?**
The Monitoring Officer as Senior Responsible Officer has oversight of:

- the integrity of the process in place within the local authority for the management of CHIS;

- compliance with Part II of the Act and with the Codes;

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

- engagement with the Office of the Surveillance Commissioner (OSC) inspectors when they conduct their inspections, where applicable; and

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

- ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the OSC.

- where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

The Deputy Monitoring Officer as the RIPA Co-ordinating Officer will:

- Maintain the central record of authorisations (see Section 8).

- Have oversight of all applications and authorisations for directed surveillance or use of CHISs, including preparation of the judicial application / order form.

- Providing general advice to investigating officers.

- Ensure a programme of RIPA training for all investigating officers and authorising officers (including the SRO) and the Co-ordinating Officer.

- Raise awareness of RIPA requirements throughout the organisation and ensuring staff are aware of the policy and receive appropriate support and training (with support from Heads of Service).

The Chief Executive, S.151 Officer and Monitoring Officer are the council's three authorising officers. Only the Chief Executive (or acting Head of Paid Service in his absence) may authorise surveillance which involves confidential information (*see*

*section 5.3*). Records of all authorisations, reviews and cancellations are to be kept by the RIPA Co-ordinating Officer.

**Performance Monitoring**
Through the review provisions set out in the policy. The Council is also monitored by the Office of the Surveillance Commissioner which inspects approximately three yearly at the current time (last inspection September 2020). The Inspector confirmed that the SRO has a strong understanding of the requirements and that a number of appropriate measure are in place which are supported by the relevant corporate policies.

It is also recommended that the Audit and Governance Committee should review the authority's use of RIPA, and the policy on an annual basis. Councillors must not be directly involved in, or have details disclosed to them of specific authorisations or engage in the authorisation process.

**Policy Consultation**
Strategic Management Team and Audit and Governance Committee

**Policy Review**
The RIPA Senior Responsible Officer will review the policy in 2025. In the interim any changes necessary to reflect updates in legislation or guidance will be made by the RIPA Senior Responsible Officer.

**Related Policies and Strategies**.
Anti-fraud, Theft and Corruption Policy
Data Protection Policy

***Note:***
The links within the policy to Forms CH1, CH2, CH3, CH4, DS1, DS2, DS3, DS4 are to the forms on the Government website. The forms are also maintained on the Policy Register under RIPA by the RIPA Co-ordinating Officer.