CORPORATE GUIDANCE DOCUMENT

THE USE AND APPLICATION OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 ("RIPA")

November 2024~~3~~

Contents

FOREWORD

This document addresses the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and its codes of practice in relation to the covert surveillance of individuals, the use of covert human intelligence sources, including undercover officers/agents/informants, and the recording of telephone conversations. This document also outlines the process governing applications for communications data.

The procedures provide a summary and overview of the legislation and codes of practice. DO NOT seek to rely on them alone. In the event of any doubt, the officer should refer to the relevant legislation or code or contact Legal Services for advice.

RIPA had effect from 1 October 2000. There are Codes of Practice that set out the authorisation procedures and records which must be followed by the County Council when undertaking investigations which fall within the scope of RIPA. The Codes of Practice were last updated in December 2022.

We are passionate about the Authority's commitment to promoting a just society that gives everyone an equal chance to learn, work and live free from discrimination. This guidance demonstrates our commitment to carry out criminal investigations in a fair and equitable manner that respects all human rights.

Enforcement activities of the Authority which fall within the remit of RIPA are subject to monitoring and oversight by the Investigatory Powers Commissioner's Office. This guidance is of particular relevance to employees conducting investigations, such as Trading Standards, Neighbourhood Protection and Fraud, as well as employees who use social media to gather information relating to individuals.

Staff should familiarise themselves with this document and the RIPA Codes of Practice. If in any doubt, guidance should be sought before undertaking any activity which falls within the scope of RIPA or which may amount to directed surveillance, even where not covered by RIPA.

Complaints made regarding activities of the Council which are within the scope of RIPA can be investigated by an independent tribunal.

Failure to follow the requirements of this guidance, of RIPA and the Codes of Practice may result in:

- Claims against the Council of alleged breaches under the Human Rights Act 1998.
- Adversely affecting the admissibility of any evidence obtained using surveillance methods.

- Compromise the safety of members of the public supplying information to the Council.

When undertaking any covert investigation, officers should have regard to the health and safety of any persons affected by the activity. Suitable and sufficient risk assessments should be undertaken and kept under review having regard to Durham Health and Safety Policy and any supplemental guidance issued by individual directorates.

The monitoring of internet and email use within the Council is regulated by The Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000. The ICT service within the Resources Directorate has software in place to monitor the use of the internet and email. If anomalies are identified, these will be investigated by the Information Security Officer in liaison with Internal Audit.

DEFINITIONS

The Act, or RIPA	Regulation of Investigatory Powers Act 2000.
Applicant	This is the officer involved in conducting an investigation or operation who makes an application electronically for the acquisition of communications data.
Authorising Officer	The person(s) designated under Sections 28 and 29 of the Act to grant authorisations for directed surveillance and the use and conduct of a Covert Human Intelligence Source, respectively. Within a Local Authority this may be a Corporate Director, Head of Service or Service Manager. The Council's Authorising Officers for RIPA are appointed by the Chief Executive. A list of the Council's Authorising Officers can be found as Appendix 1.
Communications Service Provider (CSP)	These include telecommunications, internet (including email) and postal service providers.
Conduct of a Source	Any action of that source, falling within the terms of the Act, or action incidental to it (i.e., what they do).
Confidential Material	Communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material.
Controller	In relation to a CHIS, the person or designated managerial officer responsible for overseeing the use of the source and recording this information.
Covert Human Intelligence Source (CHIS)	Commonly known as Agents, Informants, Undercover Officers. Means a person who establishes a personal or other relationship with someone else for a specified covert purpose.

Covert Surveillance	Surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.
Designated Person	This is the authorising officer for the purposes of obtaining communications data who must be registered with the National Anti-Fraud Network by the SRO. This person must not be the applicant.
Directed Surveillance	Surveillance, which is covert but not intrusive, is conducted for the purposes of a specific investigation, is likely to result in the obtaining of private information about a person and is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the Act to be sought.
Handler	An investigating officer, in relation to CHIS, having day to day responsibility for: - dealing with the source on behalf of the authority; - directing the day-to-day activities of the source; - recording the information supplied by the source; and - monitoring the security and welfare of the source.
Intrusive Surveillance	In no circumstances is the Council permitted to carry out intrusive surveillance. Covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Surveillance which is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.
IPCO	Investigatory Powers Commissioner's Office.
Private Information	This includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship

	with others, including family and professional or business relationships. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public, and where a record is being made by a public authority of that person's activities for future consideration or analysis. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.
RIPA Monitoring Officer	This is the Senior Lawyer (Commercial and Corporate Governance) who is responsible for maintaining the central register, the oversight of RIPA applications and training.
Senior Responsible Officer (SRO)	This is the ~~Head~~ Director of Legal and Democratic Services who is responsible for the integrity of the process in place within the authority for surveillance, compliance with Part II of RIPA and the Codes of Practice, oversight of reporting errors, engagement with the IPCO during and post inspections.
Tasking	An assignment given to the source, asking him or her to obtain information, to provide access to information, or to otherwise act incidentally for the benefit of the relevant public authority.
"The Use" of a source	Any action to induce, ask or assist a person engaged in the conduct of a source or to obtain information by means of an action of the source. (What they are asked to do). Surveillance includes: - monitoring, observing or listening to persons, their movements, their conversations, or their activities or communications; - recording anything monitored, observed or listened to in the course of surveillance; and surveillance by or with the assistance of a surveillance device (any apparatus designed or adapted for use in surveillance).

SECTION A - DIRECTED SURVEILLANCE UNDER RIPA

1. INTRODUCTION

1.1 Directed Surveillance means surveillance which is conducted in a manner to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. It does not include “intrusive” surveillance (consisting of monitoring people in residential premises or private vehicles) which **cannot** be carried out by local authorities.

1.2 A RIPA authorisation provides lawful authority for a Public Authority to carry out directed surveillance. RIPA authorisations may only be given where the directed surveillance is being carried out in connection with the investigation of serious criminal offences (i.e., those attracting a maximum prison sentence of six months or more or involving tobacco or alcohol sales to children).

1.3 This section deals with directed surveillance authorisations under RIPA. Where directed surveillance is required in relation to matters not attracting the protection of RIPA these are dealt with at Section F of this Guidance (social media investigations) and Section H (other directed surveillance operations that are unrelated to ‘RIPA offences’).

1.4 Therefore, if your surveillance does not relate to the criminal offences set out in paragraph 1.2 above, then not all parts of this section of the Guidance will apply and must be read in conjunction with Section F and/or Section H as applicable.

1.5 The Authorising Officers are documented in the central RIPA record held within Legal and Democratic Services. Where possible, Authorising Officers should not authorise operations in which they are directly involved i.e., where they have direct line management [or supervision] of the Applicant.

1.6 Whenever directed surveillance takes place and is for the purpose of obtaining, or is likely to obtain, private information about a person (whether or not they are the target of the operation) an authorisation should be obtained.

1.7 By obtaining an authorisation, the surveillance operation is carried out in accordance with the law and the safeguards that exist.

1.8 Prior to granting an authorisation, the Authorising Officer must be satisfied that the proposed surveillance is necessary for the prevention of crime and is proportionate to what it seeks to achieve. 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 investigation and operational terms.

1.9 Careful consideration must also be given to any community sensitivities that may be exacerbated by any individual surveillance operation.

1.10 Before applying for an authorisation, the Investigating Officer should consider whether or not the evidence sought could be obtained by alternative methods.

1.11 Where an Officer has considered whether an authorisation for directed surveillance is required and concludes it is not, this must be documented and approved by an Authorising Officer.

2. COLLATERAL INTRUSION

2.1 The officer seeking the authorisation (the Applicant) and the Authorising Officer should also consider the possibility of collateral intrusion and record their deliberations. This is private information about persons who are not subjects of the surveillance or property interference activity. Steps should be taken to assess the risk and, where possible, minimise the risk of collateral intrusion. Where unforeseen collateral intrusion occurs during an operation, the Authorising Officer must be notified, and consideration given to amending the authorisation following a review.

2.2 Consideration must also be given as to whether or not the surveillance activities of the Service take place where similar activities are also being undertaken by another agency e.g., the Police, Benefits Agency, Environment Agency.

2.3 Liaison should also be made with Durham Constabulary Local Intelligence Officers, where appropriate.

3. RECORDS OF AUTHORISATIONS

3.1 A record of all authorisations must be maintained for six ~~three~~ years from the ending of each authorisation. This should include not only those authorisations granted, but also those which are refused.

3.2 A copy of each authorisation will be maintained by the Authorising Officer within each service. The original authorisation must be supplied for the **central record** of authorisations managed by Legal and Democratic Services on behalf of the Senior Responsible Officer. The original authorisation can be provided by electronic means subject to there being a satisfactory audit trail for the document.

3.3 Authorisations must be supplied to the Senior Responsible Officer and/or the RIPA Monitoring Officer within 24 hours of the authorisation being granted~~.~~.

3.4 Due to the sensitive nature of **all documentation** covered by the Act, consideration **MUST** be given to the means by which original authorisations are forwarded to the central record to ensure confidentiality.

4. AUTHORISATIONS FOR DIRECTED SURVEILLANCE

4.1 An authorisation is required for directed surveillance undertaken:

a) for a specific investigation or operation; and

b) where the surveillance is likely to result in obtaining private information about any person (whether or not they are the subject of the surveillance).

4.2 An authorisation is **NOT** required for covert surveillance carried out as an immediate response to events or circumstances which could not be foreseen.

4.3 Authorisations do not cover covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. This activity is termed as **INTRUSIVE SURVEILLANCE CANNOT BE UNDERTAKEN BY LOCAL AUTHORITIES**. An observation post outside of premises with a limited view and no sound would not constitute intrusive surveillance. If equipment is used without the device being on the premises or in the vehicle, but which consistently provides information of the same quality as if it were, the action may qualify as intrusive surveillance. (For further guidance see Section 26 of the Act).

4.4 The use of overt CCTV surveillance systems is not normally caught by the Act, since members of the public are aware that such systems are in use. There may be occasions when public authorities use covert CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for directed surveillance may be necessary. A protocol has been produced to protect those officers responsible for such systems, which is set out in Appendix 2.

4.5 Where the surveillance activity is likely to result in Confidential Material (see Definitions section above) being obtained, the Authorising Officer within Durham County Council will be the Chief Executive or, in their absence, their Deputy. The usual Authorising Officers cannot authorise the acquisition of Confidential Material.

5. COVERT VIDEO CAMERA AND AUDIO RECORDING EQUIPMENT

5.1 This equipment is frequently employed during test purchase exercises and other monitoring activities undertaken by the Authority for the purpose of recording the transaction/activity and obtaining photographic evidence of the suspect. Concealed voice recorders may be used to record conversations without the knowledge of the other party.

5.2 The deployment of such equipment clearly has the potential for, not only obtaining personal information in relation to the suspect, but also collateral intrusion into the activities of other persons in the vicinity of the operation.

5.3 An authorisation is therefore required before using such equipment to safeguard against any challenge as to Human Rights infringements. The manner in which such equipment is used may also invoke the requirements relating to Covert Human Intelligence Sources and Part B of this Guidance should be consulted.

6. GROUNDS FOR AUTHORISING DIRECTED SURVEILLANCE APPLICATIONS

6.1 For an authorisation for directed surveillance it **must** be shown to be necessary to use covert surveillance in the investigation on specific grounds. Directed surveillance undertaken by Local Authorities can only be authorised under RIPA for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol, tobacco or nicotine inhaling products.

6.2 Directed surveillance cannot be authorised under RIPA for the purpose of preventing disorder that does not involve criminal offence(s).

7. JUDICIAL APPROVAL OF DIRECTED SURVEILLANCE APPLICATIONS

7.1 From 1 November 2012, a local authority who wishes to authorise the use of directed surveillance under RIPA must obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace (a District Judge or Lay Magistrate) before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of directed surveillance is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique as described in the application.

Further guidance on the Local Authority judicial application process, including the Council's RIPA Authorisation Procedure, can be found on the Intranet and from the RIPA Monitoring Officer.

8. DURATION OF AUTHORISATION

8.1 A written authorisation is valid for three months, unless cancelled. This begins on the day on which the Justice of the Peace approves the grant of the application, the expiry date will be considered to be three months minus one day from the date of signature by the Justice of the Peace. The time at which the authorisation is granted must also be recorded on the documentation.

9. RENEWAL

9.1 An authorisation may be renewed for a further period of three months. A renewal of a grant of a directed surveillance authorisation must be approved by a Justice of the Peace before it can take place. It may be renewed more than once, provided that the renewal continues to meet the criteria for authorisation. The number of occasions it has been renewed should be recorded. The details of any renewal should be recorded centrally.

10. REVIEW

10.1 The Authorising Officer should ensure that a system is in place to review authorisations before they cease to have effect. It is a matter for the Authorising Officer to determine how frequently a review is necessary and practicable. This must be stated within the authorisation as a **control measure.** The authorisation should also be reviewed prior to expiry to determine whether or not a renewal is required and can be justified. The Authorising Officer may make use of one of the following for example: a diary entry, work planner, MS Exchange calendar/alarm facility to generate a message prompt at least **ten** days before the expiry date.

10.2 The Authorising Officer may amend specific aspects of the authorisation upon a review, for example by discontinuing surveillance against particular persons or the use of particular tactics.

10.3 **Reviews must be presented by email or paper copy delivered to the Senior Responsible Officer and/ RIPA monitoring Officer within 24 hours of the review. Reviews must not be backdated.**

11. CANCELLATIONS

11.1 The Authorising Officer who granted or last renewed the authorisation **must** cancel it if satisfied that the directed surveillance no longer satisfies the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer, or the person who is acting as Authorising Officer.

11.2 An authorisation should also be cancelled once the activity which was the subject of the authorisation, has been completed. The authorisation should not be left to lapse as a result of the time limit expiring.

11.3 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This is required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations. It is also necessary to detail the amount of time spent on the surveillance as this is required to be retained by the Senior Responsible Officer.

11.4 The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what, if any, images were obtained and any images containing third parties. The Authorising Officer should take this into account and issue instructions regarding the management and disposal of the images etc.

11.5 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the Senior Responsible Officer This will assist with future audits and oversight.

11.6 The cancellation form will be filed by the Authorising Officer with the original authorisation in the central record of authorisations managed by Legal and Democratic Services.

11.7 **Reviews must be presented by email or paper copy delivered to the Senior Responsible Officer and/or RIPA monitoring Officer within 24 hours of the review. Reviews must not be backdated.**

12. RECORDS AND ERRORS

12.1 Material obtained as a result of surveillance activities should be recorded on the "Record of Product obtained by Directed Surveillance Form".

12.2 A copy of this form should be forwarded to the Authorising Officer to be filed with the Authorisation Form. The original should be retained by the Investigating Officer as part of the case file. Internal procedures within some departments may require that all authorisations and case materials are held within a specified secure location.

12.3 A record must also be maintained of the period over which surveillance has taken place, to assist with reviews and renewal applications.

12.4 There is a requirement to report all covert activity that was not properly authorised to the IPCO in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or was conducted beyond the directions provided by the Authorising Officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Investigatory Powers Commissioner has been followed. This will also assist with the oversight provisions of the Council's RIPA activity.

12.5 The reporting requirement does not apply to covert activity, which is deliberately not authorized, because an Authorising Officer considers that it does not meet the legislative criteria but allows it to continue. This would be surveillance outside of RIPA and further detail is set out at Section H of this Guidance.

13. HANDLING PRODUCTS FROM SURVEILLANCE ACTIVITIES

13.1 Product from Covert Surveillance activities may consist of photographs, video film, voice recordings, surveillance log, officer notes.

13.2 The above may be required as evidence in current or future criminal proceedings. Officers must have regard to the provisions of the Criminal Procedure and Investigations Act 1996 in relation to unused material. Product obtained via an authorisation may be used by the Authority in other investigations.

13.3 Although specific legislation, including data protection legislation, provide for the disclosure of information in certain circumstances, additional controls are introduced by RIPA.

13.4 The use of any product obtained by authorised surveillance activities outside of the Public Authority or the Courts should only be authorised in the most exceptional circumstances. **Joint operations should make reference to the potential use of evidence by each agency.**

13.5 Officers may receive requests from other agencies for product, which may include photographs of suspects, descriptions, and vehicle details. Where this information has been obtained under an authorisation, further guidance should be sought from the Authorising Officer and, if disseminated to an outside agency, meet the requirements of relevant data protection legislation.

14. STORAGE AND RETENTION OF PRODUCT

14.1 All material associated with an application, together with material obtained throughout a surveillance operation, will be subject of the provisions of the Criminal Procedure and Investigations Act 1996 Codes of Practice, which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of data protection legislation.

14.2 Officers should make themselves aware of the relevant data protection provisions and how they impact on the whole RIPA process. Material obtained, together with relevant associated paperwork, should be held securely and any dissemination of the product may only be disclosed to those that can lawfully receive it. The material may only be retained for as long as is necessary. Therefore, material retained outside of the CPIA provisions must have some justification to meet data protection requirements. If in doubt advice should be sought from the RIPA Monitoring Officer.

14.3 Material which is required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or, if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

14.4 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction in all other cases.

14.5 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

15. DISPOSAL OF PRODUCT

15.1 Officers should have regard to Article 5 of the GDPR and, for law enforcement purposes, section 39(1) of the Data Protection Act 2018. This provides that personal data should be kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data is processed.

15.2 Product which has been destroyed should have this fact recorded on the Record of Product Obtained by Directed Surveillance form and be signed by the Officer (See 10.0).

15.3 An amended copy of this Record form should be forwarded to the Authorising Officer, indicating destruction of the product obtained from the surveillance activity.

16. GUIDANCE NOTES FOR THE AUTHORISATION OF DIRECTED SURVEILLANCE

16.1 Does the activity involve:

The systematic covert surveillance of an individual (whether or not the identity is known) which is likely to gather personal information?

IF SO, AN AUTHORISATION IS REQUIRED

16.2 Low level activity, for example, to determine whether a premises is still trading, will not require authorisation. Surveillance carried out in response to immediate events will also not require authorisation. However, if the surveillance activity continues for any period of time, an authorisation will be required.

16.3 **The Authorising Officer must be satisfied that:**

The authorisation is necessary for the purposes of preventing or detecting criminal offences that are either punishable by at least a 6-month custodial sentence or are related to the underage sale of alcohol or tobacco.

Consideration should also have been given to alternative methods of obtaining the evidence, and why this has not or will not work or secure the best evidence.

16.4 **The Authorising Officer must also believe that the surveillance is proportionate to what it seeks to achieve and is not excessive.**

Where the identity of the subject is known to the officer, measures should also be taken to verify (where appropriate) the address under surveillance (e.g. electoral register, business rates, utility suppliers). The Authorising Officer may also wish to include some control measures within the authorisation e.g., reviews, circumstances in which the surveillance must be stopped.

16.5 The application should provide the background to the investigation, and details of other methods which have failed to provide the information being sought or why other methods are not appropriate.

16.6 The description of the activity to be undertaken should be as comprehensive as possible, describing how the surveillance will be undertaken, where it will occur and any equipment (e.g., cameras, video camera) which will be used. The Authorising Officer must know the capabilities of the equipment. The investigating officers must not employ techniques which are not permitted by the authorisation.

16.7 The information being sought should be described, together with details of how this may provide evidence of the offence or other matter being investigated. The potential for collateral intrusion should be identified and plans to avoid / minimise such intrusion.

16.8 A statement must also be included as to the likelihood of obtaining confidential information, as defined in the Codes of Practice.

16.9 If **Confidential Material** is being sought, or **is likely** to be obtained, a higher level of authorisation is required. **This authorisation can only be given by the Chief Executive (or, in their absence, their Deputy).** Further guidance should be sought if Confidential Material becomes relevant to the investigation.

16.10 Where applications for authorisation are refused by the Authorising Officer, records of the refused application must also be maintained stating the reasons for the refusal and a service number. Copies of these refusals must be sent for inclusion in the central record.

17. NECESSITY AND PROPORTIONALITY

Necessity

17.1 For interference with an individual's rights under 'Article 8' (Right to Privacy) to be necessary, the only ground on which the Council may authorise directed ~~surveillance~~surveillance.
is for the prevention or detection of a criminal offence punishable by a maximum term of at least 6 months' imprisonment or related to the underage sale of alcohol or tobacco. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described. The Authorising Officer must be satisfied that overt measures would not be likely to secure the desired result.

Proportionality

17.2 The proposed activity must be proportionate to what it seeks to achieve. The four elements of proportionality must be fully considered in an application. Both the officer seeking the authorisation and the Authorising Officer must articulate clearly why the activity is considered to be proportionate to its legitimate aim:

1. Balance the size and scope of the operation against the gravity and extent of the perceived mischief;

2. Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others;

3. Explain why the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and

4. Provide evidence of other methods considered and why they were not implemented.

18. MEMBER OVERSIGHT

18.1 Elected members of the local authority should review the authority's use of RIPA and set the policy at least once a year. This function will be overseen by Cabinet. The Council's Corporate Overview and Scrutiny Management Board will also consider internal reports on the use of RIPA on at least a quarterly basis to ensure that it is being used consistently with the Council's policy and that the policy remains fit for purpose. Members must not be involved in making decisions on specific authorisations.

SECTION B - COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

1. INTRODUCTION

1.1 This section of the guidance document deals with Covert Human Intelligence Sources, more commonly known as Undercover Officers, Informants/Agents. Authorisation is a two-stage process:

(1) to use a source;

(2) an authority for the conduct of the source.

1.2 A Covert Human Intelligence Source is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

(a) using such a relationship to obtain information, or to provide access to information to another person, or

(b) disclosing information obtained by the use of such a relationship or as a consequence of such a relationship.

1.3 The relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

1.4 Durham County Council receives complaints routinely from the public and traders regarding the alleged activities of individuals. The actions of these complainants do not generally fall within the definition of a covert source, since they are a one-off provision of information. However, a person may become a covert source if an ongoing relationship with a public authority (Durham County Council) develops, and activities described in paragraph 1.2 above are carried out.

1.5 Where the nature of the complaint relates to a matter where an officer requests the complainant to obtain further information covertly, via a relationship with another individual, this activity is likely to fall within the scope of the Act. An authorisation will therefore be required before seeking such information. By following the authorisation procedures, the Authority will also be able to seek to safeguard the identity of the source in any subsequent legal proceedings. The origin of any information from the source can be withheld, subject to acceptance by the court of the established **Public Interest Immunity** disclosure procedures. Further guidance should be sought from Legal Services on this issue to ensure that the identities of any such individuals are safeguarded in the event of any legal proceedings, tribunals or disciplinary hearings.

1.6 The Code of Practice on Covert Human Intelligence Sources relates not only to sources (which may commonly be referred to as informants) but also the activities of sources, which consist of undercover officers who establish or maintain a covert relationship to obtain information and evidence.

1.7 Before a source may be engaged, or an undercover officer deployed, the **use and conduct** must be authorised. The 'use' part of the authorisation registers the source with the Authority. The 'conduct' part addresses what the source is tasked to do. The applicant must not be the source.

1.8 In most cases, the use and conduct of a source will be restricted to a single investigation. However, situations may arise where different conducts are required as the investigation develops. Consideration should then be given to cancelling the original authorisation and seeking a new authorisation based on the new circumstances of the investigation.

1.9 The same authorisation form is used for both use and conduct. A handler and controller must also be designated as part of the authorisation process, and detailed records of the use, conduct and tasking of the source maintained.

1.10 An Authorising Officer is a person entitled to give an authorisation for the use or conduct of a source in accordance with Section 29 of the Regulation of Investigatory Powers Act 2000. A list of the Authorising Officers is held in the **central record** managed by the RIPA Monitoring Officer on behalf of the SRO. All Authorising Officers are corporate appointments and therefore can cross-service authorise.

1.11 The use of Covert Human Intelligence Sources should be necessary and proportionate to the matter being investigated.

1.12 Failure to obtain an authorisation may render Durham County Council liable to a claim of infringing the human rights of an individual and may adversely affect the admissibility of any evidence obtained by the use of covert methods employed by a source. It is also established that a Public Authority owes a duty of care to a CHIS. Failure to undertake a robust risk assessment and authorisation may also adversely affect the position of the Authority in the source suffering any harm because of the activity in which they have been engaged.

1.13 Careful consideration must be given to any potential sensitivities which may exist before deciding whether to use a CHIS in a particular community or against a particular individual.

1.14 A separate **directed surveillance** authorisation is **not** required where any surveillance device (technical equipment) is used in the presence of the covert source.

1.15 A Covert Human Intelligence Source carrying surveillance equipment **can** be invited to enter residential premises or a private vehicle. However, the CHIS **cannot install** surveillance equipment in residential premises or a private vehicle since this activity constitutes intrusive surveillance / property interference. These techniques are not available for use by Local Authorities.

2. GUIDANCE ON THE SOURCE CULTIVATION PROCESS

2.1 When seeking an authorisation for an individual to act as a covert human intelligence source, consideration needs to be made of their potential role in the investigation. Are they prepared to be a witness? Do they need to be given protection because of providing information, by means of public interest immunity? The source may also be able to provide information relating to a number of different matters worthy of investigation.

2.2 The motives of potential sources need to be considered as part of the evaluation process. Could they be motivated by rewards or revenge? The aim could be to deflect attention away from themselves towards other individuals.

2.3 Has consideration been given to building up a detailed profile of the potential source and their associates? **In all cases** a face-to-face meeting with the complainant or any other person considered as a potential source should take place. Please be aware that the individual may have needs in respect of language, hearing or sight.

2.4 Directed surveillance may be needed to evaluate the source. Consideration should be given in certain circumstances to carrying out checks on the source with the Police. A thorough risk assessment must be carried out on the potential source, and the proposed conduct.

3. MANAGEMENT OF SOURCES

3.1 Tasking is the assignment given to the source by the handler/controller asking the source to obtain information or to take action to obtain information.

3.2 All authorisations **should be in writing** and in place before tasking a source. Every source must have a designated handler and controller.

4. DESIGNATED HANDLERS AND CONTROLLERS FOR THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

4.1 Where the Covert Human Intelligence Source is a complainant or an informant, the Handler will be the Investigating Officer and the Controller will be their line manager. Where the Covert Human Intelligence Source is an Officer of the Authority acting in

an undercover capacity, the Handler will be the Officer's line manager and the Controller will be another manager within the Service. This arrangement will ensure that an Officer does not act as a Controller and Authorising Officer thereby ensuring a level of independent scrutiny.

5. SECURITY AND WELFARE OF SOURCES

5.1 A source has no licence to commit crime. In certain circumstances it may be advisable to provide written guidance to the source, explaining what is being requested of them and the limits of the tasking. The source should be asked to sign such a document to confirm that they understand the terms of reference.

5.2 A public authority deploying a source, should consider the safety and welfare of the source when carrying out any actions in relation to the authorisation or tasking. The foreseeable consequences of the tasking should also be considered.

5.3 A Risk Assessment should be undertaken to evaluate the source and to determine the risk to the source of any tasking and the likely consequences should the identity and role of the source become known to the ~~subject~~subject, or others involved with the subject. Appropriate documentation is contained on the intranet and further information can be obtained from the RIPA Monitoring Officer.

5.4 A Handler is responsible for: dealing with the source on behalf of the Authority; directing the day-to-day activities of the source; recording the information supplied by the source; and monitoring the security and welfare of the source. The Handler should draw to the attention of the Controller:

- the Risk Assessment
- the Conduct of the Source
- the Safety and Welfare of the Source.

5.5 Where a source is known or suspected of being involved in crime, consideration should be given to their motives in supplying information. It may also be a prudent step in the management of such a source to have two officers present during any meetings with the source. Background checks on the potential source via the Police Local Intelligence Officer should also be considered.

5.6 Special provisions exist for the conduct in use of juvenile sources (under 18)~~.~~.

5.7 A source aged under 16 cannot be engaged to use a relationship with any person having parental responsibility for them. A source under 16 must have an appropriate adult present during any meetings and a risk assessment must also take place before granting or renewing an authorisation for the conduct and use of a source

under 16. This will take account of physical and psychological risks. For detailed guidance see the Regulation of Investigatory Powers (Juveniles) Order 2000.

5.8 Special consideration should also be given to the use of vulnerable individuals as a source. This will require the highest level of authorising officer, the Chief Executive. Further guidance can be found in the Code of Practice.

5.9 When granted, authorisations for juvenile sources, i.e. a source under the age of 18, have effect for one month. Juvenile source authorisations should be issued by the highest level of authorising officer in an Authority, this is the Chief Executive of Durham County Council.

6. JUDICIAL APPROVAL OF CHIS APPLICATIONS

6.1 From 1 November 2012, a local authority who wishes to authorise the use of a CHIS must obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace (a District Judge or Lay Magistrate) before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of a CHIS is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique as described in the application.

7. DURATION OF AUTHORISATIONS

7.1 Authorisations have effect for a period of twelve months from the date of judicial approval, unless a juvenile, in which case the authorisation has effect for a period of one month. The Authorisation should be managed and be made subject to reviews set as a control measure by the Authorising Officer.

7.2 Records of authorisations are to be retained for a minimum period of one year to comply with the Code. However, it will be policy to retain the records for a period of six years to safeguard against any civil claims against the Authority, including those under the Human Rights Act 1998, where limitation is one year with the court able to exercise discretion to disapply limitation, and data protection claims where limitation is six years.

7.3 Destruction of the authorisation form should be documented in the Authorising Officer’s Management Record file.

8. RENEWALS AND REVIEWS

8.1 An authorisation may be renewed, after the Authorising Officer reviews the use made of the source having regard to:

a) the tasks given to the source; and
b) the information obtained from the source.

If satisfied that the original authorisation criteria continue to be met, a renewal may be authorised. A renewal of a grant of a CHIS authorisation must be approved by a Justice of the Peace before it can take place.

8.2 Since an authorisation for a CHIS may remain in force for a period of twelve months, regular reviews should be undertaken to ensure the ongoing validity of the activity and the ongoing welfare and security of the source. Any changes to circumstances may require that further risk assessments are undertaken.

8.3 The reviews should be undertaken at intervals of no longer than three months and documented. Additional control measures may also be introduced as a result of a review. The Authorising Officer should implement a system to identify appropriate review dates (e.g., the MS Exchange Calendar alarm option).

9. CANCELLATIONS

9.1 An Authorising Officer must cancel an authorisation where:

- the use or conduct of the source no longer meets the original authorisation criteria; or
- the procedures for managing the source are no longer in place.

Where possible, the source should be informed of the cancellation, and this fact noted on the cancellation.

9.2 Where an investigation no longer requires the authorisation to be in place e.g. the evidence has been obtained, it should be cancelled promptly rather than allowed to expire through time, and the reason for cancellation documented.

9.3 **Cancellations must be presented by email or paper copy delivered to the Senior Responsible Officer and/or RIPA monitoring Officer within 24 hours of the cancellation. Cancellations must not be backdated.**

10. SOURCE RECORDS

10.1 Records of use of the source, and the product provided by the source, should be maintained by the service for a **period of six years**. Records should not be destroyed without the authority of the Authorising Officer. Destruction of records should be documented in the Authorising Officer's Management Records file.

10.2 The following information must be recorded:

- Authorisation Reference Number
- Authorising Officer
- Identity used by Source (if any)
- Identity of Source
- Reference used in the authority to refer to Source (if any)
- Information relating to security and welfare of Source ○ A record that any risks to the security and welfare of the Source have been explained to and understood by the Source
    - Records of reviews conducted on the continuing use and welfare of the Source
    - The date when the Source was recruited
    - The circumstances of the recruitment
- Identity of the Handler and Controller (and details of any changes)
- A record of the tasks and activities given to the Source
- A record of all contacts or communications between the Source and a person representing the Authority
- The information obtained through the Source
- How the information is used
- A statement as to whether any payment, benefit or reward is provided by or on behalf of any investigating authority and details of it
- Reasons for cancelling / not renewing the authorisation and the date and the time of such a decision.

10.3 It is **NOT** Durham County Council policy to directly offer any benefits or rewards to a CHIS. Rewards may be forthcoming from a third party e.g., from a trade association or trademark holder where an investigation involves counterfeit goods.

11. THE APPLICATION FOR AUTHORISATION

11.1 The application must include the following:

- The grounds on which the authorisation is sought and why it is necessary (preventing or detecting crime or preventing disorder).
- A detailed explanation of the proportionality of the Use/Conduct.

- Where the matter relates to a specific investigation, details of that investigation or operation.
- Details of the purpose for which the source will be tasked.
- Details of what the source will be tasked to do.
- Details of the level of authority required, having regard to any confidential material that might be obtained as a consequence of the authorisation (this will invoke the requirement to be authorised by the Chief Executive if confidential material is being sought or is likely to be obtained).
- Details of who will be affected and plans to avoid/minimise collateral intrusion. Where this changes, the Authorising Officer must be ~~informed~~informed, and the authorisation reviewed.
- A detailed Risk Assessment must have been undertaken. A review may also be required if the assessment is not current.
- The Authorising Officer may wish to impose control measures on the authorisation that is granted.

11.2 Unless renewed or cancelled, an authorisation remains in force for 12 months from the date of judicial approval (one month for juveniles). The authorisation should be given a unique operation reference number and be recorded in the management record file. Conduct authorisations should be referenced to the original use authorisation.

11.3 A duplicate/copy of the authorisation should be issued to the officer. This will ensure that the officer has a record of the scope of the activity authorised.

11.4 Applications which are refused should also be recorded, together with the reasons for the refusal and a service number. Copies of these refusals must be sent for inclusion in the central record.

12. ERRORS

12.1 There is now a requirement to report all covert activity that was not properly authorised to the IPCO in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the Authorising Officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Investigatory Powers Commissioner has been followed. This will also assist with the oversight provisions of the Council's RIPA activity.

SECTION C - RISK ASSESSMENTS

1. Whenever undertaking covert directed ~~surveillance, or~~surveillance or engaging in the conduct and use of a Covert Human Intelligence Source, the proposed activity must be the subject of a suitable and sufficient risk assessment and evaluation of the proposed Source.

2. Directed Surveillance activities clearly have the potential to expose staff to hazards should their activities become known to the subject or even to others during the operation. The use of Covert Human Intelligence Sources has the potential to expose handlers, undercover officers, agents/informants and the public to health and safety risks. A duty of care may also lie with officers and the Authority in managing sources.

3. Authorising Officers, Controllers, Handlers, Undercover Officers and Investigating Officers must all have regard to Durham County Council's Corporate Policy on Health and Safety. This addresses issues such as lone working and violence to staff.

4. The Policy states that, *"Durham County Council will ensure that management systems are produced that are sufficient to effectively identify, assess, manage and control the risks to the health and safety of employees and other people affected by their work"*.

5. It is a matter for each Service to determine the training required to ensure that staff are competent to undertake risk assessments of proposed operations/use of covert sources. All incidents/dangerous occurrences during the course of operations should be reported in accordance with the corporate Health and Safety Procedures.

6. Consideration should also be given to staff training requirements to engage in covert activities, surveillance and acting in an undercover capacity.

7. This section of this guidance document is intended to provide an overview, which must be borne in mind when undertaking surveillance.

8. Further Guidance on Health and Safety issues is available from:
    - The Management of Health and Safety at Work Regulations 1999
    - The Corporate Health and Safety Policy Document and Guidance
    - The Health and Safety Unit (tel. 03000 261016)

9. Risk assessments for directed surveillance operations should be undertaken by the officer in charge of the proposed activity and submitted with the authorisation application.

10. Risk assessments for the use of a CHIS should be undertaken by the Handler and considered by the Controller as part of a risk management process. The assessment should then be forwarded to the Authorising Officer with the application.

11. The assessment should consider the Ethical, Personal and Operational Risks of the proposed activity. The evaluation of a potential source is an important part of the application process.

12. Risk assessment is not a one-off activity but an ongoing process throughout the operation and use of the source, since circumstances may change, and a review may be required.

13. The nature of the risks surrounding the deployment and management of individual sources, handlers and operational activities will vary according to a wide range of factors on a case-by-case basis. Risk assessment allows the handler and controller to advise the Authorising Officer of the plan for managing the risks.

14. Authorising Officers will not authorise a Directed Surveillance operation or the use of a source without evidence that the risks have been considered and a plan for their management.

SECTION D - RECORDING OF TELEPHONE CONVERSATIONS

1. The interception of communications sent by post or via public or private telecommunications systems attached to the public network may only be authorised by the Secretary of State (Part I Regulation of Investigatory Powers Act 2000).

2. The attachment of a surveillance device to a telecommunications system can only be undertaken under a warrant issued under Section 5 of the Act. This is a power which does not extend to local authorities.

3. An exception to the rule requiring a warrant exists where one party to the conversation consents and an authorisation for directed surveillance is obtained, as set out at section 48(4) of the Act.

4. For example, a member of the public may consent to the recording of a telephone conversation made by or to them. An officer may seek to record such a conversation to assist with an investigation into another person's activities.

5. An officer may also request a colleague to telephone another person as part of an investigation or may make the call themself. These situations may require an authorisation to be granted if the RIPA criteria are met.

6. Officers considering making a test purchase must be very careful when deciding whether the recorded conversation is to obtain goods, or whether it is to gather information which will only be obtained in a covert capacity.

SECTION E - ACCESSING COMMUNICATIONS DATA

1. WHAT IS COMMUNICATIONS DATA

1.1 This section of the guidance document details the system in place where an investigating officer seeks to obtain communications data within the scope of their enquiries. In June 2019, the Investigatory Powers Act 2016 came into force which changed the procedure for applications relating to communication data. A code of practice has also been published for communication which can be found here.

1.2 There are two categories of data which are entity and event.

1.3 Entity data covers information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. This means that individual communication devices such as phones, tablets and computers are entities.

1.4 Examples of entity data include:

- 'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?"; subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information about selection of preferential numbers or discount calls.

1.5 A communications data authorisation cannot authorise an authority to use a password obtained through that or another communications data authorisation. If the authority wishes to use a password obtained through a communications data authorisation to access the content of stored communications or any communications service it must, in accordance with section 6 of the Act, ensure that it has appropriate lawful authority.

1.6 Events data covers information about time-bound events taking place across a telecommunication system at a time interval. Communications data is limited to communication events describing the transmission of information between two or

more entities over a telecommunications service. This will include information which identifies, or appears to identify, any person, apparatus or location to or from which a communication is transmitted. It does not include non-communication events such as a change in address or telephone number for a customer.

1.7 Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been, or may be, made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and email headers) to the extent that content of a communication, such as the subject line of an email, is not disclosed;
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

2. APPLICATIONS FOR COMMUNICATIONS DATA

2.1 All applications to obtain communications data are to be made through the National Anti-Fraud Network (NAFN). As a local authority, an Applicant who wishes to acquire communications data under the Investigatory Powers Act 2016 must work with the NAFN Single Point of Contact (SPoC) throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner. The requirement for Judicial Approval for a local authority for applications for communications data has been removed. There is independent authorisation by the Office for Communications Data Authorisations (OCDA).

2.2 In addition to being considered by a NAFN SPoC, the authority making the application must ensure someone of at least the rank of the Senior Responsible Officer is aware that the application is being made before it is submitted to an authorising officer in the OCDA. The local authority Senior Responsible Officer must be satisfied that the

officers verifying the application are of an appropriate rank and must inform NAFN of such nominations.

2.3 The introduction of the Office for Communications Data Authorisations (OCDA) means the acquisition of communications data by Durham County Council officers is no longer subject to judicial approval by a magistrate. An officer can make an application online and, once this application has been approved by NAFN, the data is released. There is no involvement of legal services in this process. There is a requirement for an officer making an application to ensure someone of at least the rank of the Service Manager is aware the application is being made before it is submitted to OCDA.

3. RECORDS AND ERRORS

3.1 Records of all applications, authorisations, notices, cancellations and refusals must be maintained since an inspection regime by the Interception of Communications Commissioner's Office is established under this part of the legislation, making Council procedures and documentation subject to periodic inspection by an external body. These records are held by NAFN.

3.2 Where any errors have occurred in granting authorisations or notices (e.g., subscriber details of an incorrect telephone number being obtained), or more data has been supplied by the CSP than that requested, i.e., obtaining excess data, a record must be kept, and the matter reported to the Interception of Communication Commissioner's Office as soon as practicable. A copy of the error record must also be provided to NAFN, the SRO and the RIPA Monitoring Officer. The SRO and RIPA Monitoring Officer will ensure that this is recorded on the central register.

3.3 Further guidance on NAFN and Communication Data can be obtained from the Authorising Officer.

SECTION F - PROCEDURE FOR THE USE OF SOCIAL MEDIA IN INVESTIGATIONS

1. INTRODUCTION

1.1 This procedure concerns the use and monitoring of social media by officers in the course of their duties. It should be read in conjunction with other appropriate sections of this Guidance, and with the Council's Policies on the Personal Use of Social Media, Information Security and Social Media.

1.2 The Human Rights Act 1998 provides that everyone has the right to a private life, which shall only be interfered with by public authorities when lawful, necessary and proportionate. It applies when officers are using social media.

1.3 People have a reasonable expectation of privacy that applies even to the information they post on social media without privacy settings. Care should be taken by officers not to unnecessarily infringe that expectation. This guidance sets out the matters to be considered in striking that balance, how to obtain authorisation to use social media, and how social media should be used.

Levels of Engagement

1.4 There are 5 'levels' of social media engagement to think about:

- General internet searches: no authorisation needed;
- 'Drive-by' visits to social media profiles: Access authorisation may be needed;
- Monitoring visits for 'non-serious criminal offence' purposes: Directed Surveillance authorisation needed;
- Monitoring visits relating to more serious offences: RIPA (Directed Surveillance) authorisation needed;
- Befriending people for covert purposes: RIPA (CHIS) authorisation needed.

1.5 A preliminary examination of the internet to see if someone has an online presence is unlikely to engage their right to privacy. However, if that search reveals a presence on social media sites, then an authorisation (in some form) ~~will always~~ may be needed to interrogate those sites.

Summary of Social Media Authorisations

1.6 There are four types of ~~authorisation~~authorisations that may be required, as follows:

(i) Access authorisation

This is where an officer is making an initial examination of an individual's online profile to establish whether they are of relevance to an investigation, but without any intention of extracting or recording any information. Line Manager authorisation is required and should be recorded on the relevant case file.

(ii) Non-RIPA directed surveillance authorisation

This is where an officer wishes to access a social media site with the intention of monitoring, extracting or recording the information found there. These types of activity are (generally speaking) 'directed surveillance'. Where the purpose of the visit is other than to investigate serious criminal offences (those resulting in maximum sentences of at least 6 months' imprisonment or involving the underage sale of tobacco or alcohol), they cannot be authorised by the Magistrates under RIPA. However, they can be just as intrusive as RIPA surveillance (and potentially, if less serious or no criminal offences are involved, a more disproportionate privacy interference) and so need to be authorised internally by a Tier 4 Manager or, for surveillance of the Council's staff, the relevant Head of Service in conjunction with the Head of Internal Audit. An Authorising Officer should always be consulted. For further guidance see Section H.

(iii) RIPA directed surveillance authorisation

As above but involving investigation of the more serious offences allowing a RIPA authorisation to be obtained from the Magistrates. Where it is available, a RIPA authorisation must always be obtained. For further guidance see Section A.

(iv) CHIS authorisation

This is where Covert Human Intelligence Source profiles are set up to establish a relationship with the subject, and an authorisation under RIPA is required. For further guidance see Section B.

2. USE OF COUNCIL ACCOUNTS

2.1 Officers must on no account use their own personal social media accounts in order to investigate or interrogate other social media profiles in the course of their work. Each Service will have its own social media accounts for this purpose.

2.2 Some of these accounts will be ‘fake’ and some will be ‘open’ Council accounts.

2.3 A ‘fake’ or covert account is used when it is necessary to view the profile of another social media user without the subject knowing that the Council is viewing their information. A ‘fake’ profile with a pseudonym should be used to protect the identity of the investigating officer and the integrity of an investigation. Approval from an Authorising Officer is required before this type of profile can be used.

2.4 An ‘open’ or overt account is used when seeking to advise the subject as to legal requirements, issue a warning as to their conduct or to obtain information from them. ‘Open’ accounts must be created with a pseudonym which makes clear that Officers of Durham County Council are seeking to contact people via social media platforms.

2.5 Access Authorisations will usually only be granted where ‘open’ Council accounts are used to access the ‘open’ subject social media site.

2.6 Directed Surveillance Authorisations (whether RIPA or non-RIPA) may use either type of account, but greater justification may be required to use a fake account. The use of a ‘fake’ social media profile MUST be approved by one of the Council’s Authorising Officers.

2.7 Fake accounts will inevitably be used in CHIS cases, which may also involve seeking to access the subject account where privacy settings have been applied.

3. WHETHER ‘ACCESS’ OR DIRECTED SURVEILLANCE

3.1 Section 26 of the Regulation of Investigatory Powers Act 2000 defines what is meant by ‘private information’ and by ‘directed surveillance’.

3.2 **Private information**, in relation to a person, includes any information relating to his or her private or family life. Private information will inevitably be obtained as a result of accessing anyone’s personal social media profile, although not necessarily a business’s account. The important point is that, just because an individual may have published this information on an open source, does not stop it being ‘private information’.

3.3 **Directed surveillance** is surveillance that is:

(1) Covert. Surveillance is covert if it is carried out in a manner calculated to ensure that the subject of it is unaware that it is taking place. Unless the Council Service has explicitly drawn to the person's attention that they are likely to be the subject of social media monitoring or investigation, the Council's view is that monitoring their social media sites is going to be covert surveillance. They would not otherwise reasonably expect it to ~~happen, or~~happen or be aware that it is happening.

(2) In order to be 'directed surveillance', the surveillance is undertaken for the purpose of a specific investigation or operation, in a way that private information is likely to be obtained and is not an immediate response to circumstances meaning an authorisation is not reasonably practicable.

3.4 Purpose of site visit

It is not always easy to decide when visiting a social media site becomes directed surveillance, and so the Council requires any social media visit to be authorised even at a 'reconnaissance' or 'access' level. The general distinction is that, if you are looking just to see if something is there, then that is not directed surveillance but merely reconnaissance, but, if you are watching the space and collecting information, then it will be directed surveillance. Another way of putting it might be that, if you are going onto the site hoping to extract any information that you could then use as evidence in any way, it is likely to be directed surveillance~~.~~.

The Home Office Code of Practice on Covert Surveillance and Property Interference of December 2022 sets out factors to consider in establishing whether a directed surveillance authorisation is required. These include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s); and
- Whether it is likely to involve collateral intrusion, i.e. identifying and recording private information about third parties who might be referenced on, or have posted to, the site.

3.5 Social Media Authorisation Assessment Form

When Officers are assessing if a RIPA or Non-RIPA authorisation is required in order to capture information on a social media account, the Council's Social Media Authorisation Assessment needs to be completed.

The purpose of this document is for Officers to assess the Subject's reasonable expectation of privacy and whether the material available is private and not merely trivial or anodyne information. The form also requires Officers to assess the information against the factors contained within the Home Office Code of Practice.

To help assist Officers an example form is available on the Council's Intranet.

~~3.5~~3.6 Examples

The Code of Practice gives the following examples (paraphrased where appropriate):

An officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

An officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit.

An authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance operation. Similarly, general analysis of data for predictive purposes is not usually directed surveillance. In such cases the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of

surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that an authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

4. ACCESS AUTHORISATIONS

4.1 If an officer is satisfied that visiting a social media site will not amount to directed surveillance, then an Access Authorisation must nevertheless be sought from a line manager. The recommended form for requesting such authorisation is set out at Appendix 3 to this Guidance~~—~~.

4.2 Officers must briefly set out why it is considered that access to the site is necessary and proportionate to their investigation. Line managers must only grant authorisation if satisfied that a directed surveillance authorisation is not required, and that the reconnaissance visit is justified~~—~~.

4.3 This is not meant to be a burdensome process but a relatively quick 'sense check' second opinion to confirm the line manager's agreement that no privacy interference will take place. The authorisation may be recorded by electronic means without the need fora 'wet' signature.

4.4 A record of the authorisation should be retained on the relevant matter file (and subject to the same retention policy)~~—~~.

4.5 Accessing the relevant social media account or profile should take place within 10 working days of the line manager's authorisation of it.

5. DIRECTED SURVEILLANCE

5.1 Where an investigation or operation will involve accessing social media sites that may result in obtaining private information about a person (whether or not that is the purpose of accessing the site), then a directed surveillance authorisation, whether RIPA or non-RIPA, ~~will~~ may be required.

5.2 Non-RIPA directed surveillance may be authorised by Tier 4 Managers or Heads of Service. However, one of the RIPA Authorising Officers (set out at Appendix 1) must always be consulted before that management consent is given. A written record of the consultation should be sent to Legal Services to be stored on the electronic case management system.

Difference between RIPA and non-RIPA surveillance

5.3 The distinction between RIPA and non-RIPA lies, not in how the surveillance is undertaken but, in its purpose. Directed surveillance undertaken as part of an investigation into serious criminal offences, or underage tobacco or alcohol sales, should be authorised by a Magistrate under RIPA. When so authorised, the intrusion is deemed lawful for all purposes. For example, any evidence so collected will be immune from any later challenge as to its admissibility in court.

5.4 Directed surveillance resulting in evidence gathered in relation to less serious offences, or in relation to matters which are not offences at all, cannot be authorised under RIPA. That does not necessarily mean it is unlawful, but it cannot attract the blanket protection of RIPA. Therefore, it can be subjected to later admissibility challenges, or perhaps Human Rights challenges on the grounds of unwarranted intrusion. It is therefore vital to have an authorisation procedure that allows the Council to demonstrate that it has considered the lawfulness and proportionality of its actions when deciding to obtain evidence in this way.

Purposes of the surveillance

5.6 Much of the guidance in Section A ("Directed Surveillance") of this Guidance will apply whether the surveillance is to be authorised under RIPA or outside of RIPA. The non-RIPA considerations set out at Section H may also apply.

5.7 The lawful purpose of the surveillance must be identified. This may be the prevention or detection of crime, or public disorder, or it may be for the purpose of protecting children or vulnerable adults, or for another of the Council's functions.

5.8 An authorisation under RIPA could only be obtained (by any public authority) where the surveillance is considered necessary on one of the following grounds:

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified by an order made by the Secretary of State.

5.9 Therefore, non-RIPA authorisations are unlikely to be granted for any surveillance that is not also for one of those purposes.

5.10 The need for, and the proportionality of, the surveillance must be assessed and found to be justified. The seriousness of the intrusion into the subject's privacy must be balanced against the need for the surveillance in terms of the investigation or operation.

Alternative options and collateral intrusion

5.11 If the evidence sought could be obtained by other overt or less intrusive methods then this must be considered preferable. The potential for collateral intrusion must be considered, and steps taken where possible to minimise that risk. The authorisation should record these considerations. Please refer in particular to paragraphs 2 and 17 of Section A to this guidance.

Authorisation Forms

5.12 The form for requesting and granting authorisation for non-RIPA Directed Surveillance is available on the intranet. The existing RIPA forms and procedure, as

set out in Section A of the Corporate RIPA Guidance, should continue to be used for RIPA surveillance applications.

5.13 'Wet' signatures by the Authorising Officer are no longer required in respect of RIPA authorisations. For non-RIPA cases, the relevant Tier 4 Manager or Head of Service's wet signature are also no longer required. In all cases, authorisations where a wet ink signature is not provided, require an electronic signature with a satisfactory audit trail evidencing the authorisation~~—~~.

6. COVERT HUMAN INTELLIGENCE SOURCES

6.1 Any CHIS authorisation requires judicial ~~approval~~approval, and such approval should therefore be sought. There is no 'non-RIPA' CHIS approval process, unlike for directed surveillance.

6.2 A CHIS exists if a person:

establishes or maintains a personal or other relationship with another person for the covert purpose of either:

(i) using that relationship to obtain information; or

(ii) covertly disclosing information obtained as a result of that relationship.

6.3 A CHIS is therefore most unlikely to arise merely by viewing someone's social media profile, even if that is done from a 'fake' Council account. A CHIS relationship could arise however if a fake profile is then used to establish a relationship with someone to elicit information about, for example, 'knock-off' goods for sale.

6.4 Merely using a 'fake' account to try to buy goods through internet trading organisations will not require a CHIS authorisation. However, it is required where a covert relationship is likely to be formed. A common example will be when liaising on Facebook with the seller directly, and the officer conceals their true identity or reasons for purchasing.

6.5 The relevant authorisation forms and procedures for CHIS applications are those already in use, as set out in Section B of this Guidance.

Records

6.6 The Online Investigation Pro-Forma will be maintained as a secure document on a restricted access Sharepoint site, with sub-sites being set up for the use of individual teams. Each sub-site will be restricted to the following:

- Tier 4 manager

- Manager
- Line manager / team leader
- Employee conducting the investigation

6.7 Employees will be responsible for updating the online investigation form, while managers will be responsible for maintaining:

- A spreadsheet recording the creation and operation of profiles (including assignment of profiles and passwords),
- Oversight of investigations,
- Maintenance of profiles (legend, password changes after each deployment etc).

6.8 Under RIPA CHIS management procedures, the above officers will also act in the roles of Handler, Controller and Authorising officer, which roles will be documented in compliance with the requirements of RIPA.

7. DO AND DO NOT

- **DO NOT** use personal social media profiles for work-related activity.
- **DO NOT** create your own profiles or email accounts for work-related activity.
- **DO NOT** befriend other profiles to obtain information without a CHIS authorisation.
- **DO NOT** change passwords of the Service Profile or the associated email accounts.
- **DO NOT** share passwords with other staff. Passwords must only be issued and changed by managers.
- **DO NOT** make use of the profiles or email accounts without prior authorisation.
- **DO NOT** link the Service Profile with any mobile devices without authorisation.
- **DO** be aware that any information you obtain in a personal capacity from any social media presence that is then used for work-related purposes will amount to unauthorised CHIS activity.
- **DO** consider your safety and that of others. Be aware of any social media activity that you conduct in your personal life and ensure that any associations or postings in the online world do not impact on the health and safety of you or your family or compromise your work role or that of colleagues.
- **DO** speak with your manager if in any doubt about whether your actions in a work or private capacity may have resulted in obtaining information about criminal activity as a result of online relationships.
- **DO** discuss any concerns or problems with your manager.

SECTION G - JOINT AGENCY SURVEILLANCE

1. In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

2. Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application form to carry out the activity. When staff are operating on another organisation's authorisation, they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Monitoring Officer. This will assist with oversight of the use of Council staff carrying out these types of operations.

SECTION H - NON-RIPA SURVEILLANCE

1. Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can only obtain an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

2. Nevertheless, surveillance may sometimes be required which falls outside of RIPA (for example in the case of anti-social behaviour offences which do not attract a maximum custodial sentence of at least six months imprisonment, or in the case of monitoring for child protection purposes). Such surveillance would still potentially infringe a person's Human Right to privacy. It is therefore essential for decisions to undertake any surveillance activities to be properly justified and documented, and to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA. This activity will be periodically reviewed by the SRO. The SRO will therefore maintain an oversight of non-RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The RIPA Monitoring Officer will maintain a central record of non-RIPA surveillance.

3. A non-RIPA surveillance application form should be completed and authorised by at least a Tier 4 level Manager. A copy of the non-RIPA surveillance application form can be found on the Intranet or is available from the RIPA Monitoring Officer.

4. Non-RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance Application Form and authorised by the Head of Service in consultation with the Head of Internal Audit. A central record of staff surveillance is also maintained by the SRO.

5. The considerations at Section A of this Guidance will largely apply to non-RIPA surveillance applications. Section A mostly applies in its entirety save for the sections dealing with the judicial approval process. The main differences between RIPA and non-RIPA surveillance are:

   (a) RIPA surveillance must be authorised judicially;

   (b) RIPA surveillance can only be protected by judicial authorisation in the case of serious criminal offences;

   (c) Authorising Officers for RIPA are set out in Appendix 1 to this Guidance. Non-RIPA surveillance may be authorised by Tier 4 Managers after consulting with an Authorising Officer, except where staff surveillance is involved where a Head of Service and the Head of Internal Audit's authorisation is required;

(d) The provisions of Section A concerning duration, renewal, review and cancellations (paragraphs 8 - 11) should be read as though the Tier 4 Manager or Head of Service substitutes for the Authorising Officer;

(e) All the requirements of Section A as to justification and record-keeping will apply.

6. The provisions of Section C of this Guidance, relating to Risk Assessments, will also apply to non-RIPA surveillance applications.

7. Where the non-RIPA surveillance is limited to investigations of a person's social media presence, then Section F of this Guidance also applies.

SECTION I - AUDITING OF AUTHORISATIONS AND RECORDS

1. Periodic audits will be carried out across relevant services, including the Central Record. These will be conducted by Internal Audit in line with the Council's Risk Based Strategic Audit Plan. This may require some material to be sanitised to maintain the safety of sources.

2. The following should fall within the scope of the audit:
   - Applications
   - Authorisations
   - Risk Assessments
   - Reviews
   - Renewals
   - Cancellations
   - Records of Product of Directed Surveillance
   - Source records
   - Staff Awareness e.g., training, memos, emails, meetings
   - Access to and awareness of the codes of practice.

3. The audit should seek to establish compliance of the authorisations / renewals / reviews / cancellations and records with RIPA, the Codes of Practice and this Guidance Document.

SECTION J - COMPLAINTS

1. The Codes of Practice on Covert Surveillance and Property Interference and Covert Human Intelligence Sources can be made available at the public offices of Durham County Council departments undertaking activities which are within the scope of RIPA.

2. The Investigatory Powers Tribunal (IPT) exists to investigate complaints about conduct by various public bodies under RIPA.

   The Tribunal can be contacted at:

   The IPT, PO Box 33220, London, SW1H 9Z

   Telephone: 0207 035 3711

   Online: www.ipt-uk.com

SECTION K - MANAGEMENT RECORDS

1. The Authorising Officer must keep a copy of the relevant documents to check against the cancellation. These documents must be kept in a secure place with restricted access. Original authorisations (including refusals), reviews, renewals and cancellations must be provided to the Central Record for Durham County Council. This is managed by the RIPA Monitoring Officer in Legal and Democratic Services. Officers forwarding confidential material to the Central Record must ensure that it is forwarded with a secure method.

2. The Central Record is held in a locked filing cabinet and on the electronic case management system for Legal Services with restricted access. The following officers have sole access to the central record:

   - The Corporate Director of Resources
   - The ~~Head~~ Director of Legal and Democratic Services (SRO)
   - The RIPA Monitoring Officer (and support officer).

3. The Record Retention Period is six years.

APPENDIX 1

Authorising Officers for the Purposes of Directed Surveillance and CHIS

Authorising Officer	Rank
Tracy Henderson	Chief Internal Auditor and Corporate Fraud Manager, Resources
Ian Hoult	Neighbourhood Protection Manager, Neighbourhoods and Climate Change
Owen Cleugh	Public Protection Manager, Neighbourhoods and Climate Change
Gary Carr	Strategic Regulation Manager
Ian Harrison	Business Compliance Manager
Tracey Johnson	Community Safety Manager

Authorising Officers for the Purposes of Communications Data

Designated Person	Rank
Tracy Henderson	Chief Internal Auditor and Corporate Fraud Manager, Resources
Paul Gibbon	Fraud Manager, Resources
Owen Cleugh	Public Protection Manager, Neighbourhoods and Climate Change

APPENDIX 2

DURHAM COUNTY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

CCTV SYSTEM PROTOCOL

1. Introduction

1.1 Durham County Council operates and manages a number of Surveillance Cameras and Closed-Circuit Television Systems (CCTV) for the purposes of monitoring public open space to deter anti-social behaviour, preventing and detecting crime and to monitor council buildings, vehicles and premises for security reasons.

1.2 It is recognised that CCTV systems may be employed to observe and record the activities of individuals, which clearly has implications under the Human Rights Act 1988 and the Regulation of Investigatory Powers Act 2000 (RIPA) in terms of intrusion into the privacy of individuals.

1.3 This protocol is a separate document to the Council's CCTV Policy and Code of Practice produced by Durham County Council in response to the code of practice issued by the Information Commissioner to ensure compliance with the Data Protection Act 2018. Officers seeking to make use of CCTV systems and recordings should, however, have regard to the requirements of the Council's policy.

1.4 This protocol serves to establish safeguards for the potential use of CCTV systems to specifically target individuals to observe and/or record their activities. Such planned activities will fall within the scope of Directed Surveillance and are subject to the controls established by RIPA to ensure that the activity is necessary, proportionate and authorised by a suitable senior officer of the Authority.

1.5 Durham County Council is committed to promoting a just society that gives everyone an equal chance to learn, work and live free from discrimination and prejudice. This protocol demonstrates our concern for human rights, and therefore contributes to our diversity agenda.

2. Authorised Activities

2.1 General, non-directed recording of events and people through the use of overt CCTV systems will not infringe the rights of the individual. This activity does not, therefore, need to be authorised through the RIPA process.

2.2 The retrospective viewing of CCTV footage to gain evidence of actual or potential criminal activity does not fall within the definition of covert surveillance and would, similarly, not require any form of authorisation. An approach should be made to the County Hall Facilities Manager for permission to view. Similarly for sites other than County Hall, the officer in charge of the premises should be approached in the first instance.

2.3 The processing of such data is, however, subject to the Information Commissioner's Code issued under relevant data protection legislation.

2.4 Provision also exists within the RIPA framework to react to immediate events without the need to obtain an authorisation. For example, should a CCTV operative witness an attempted break-in of any property, it would be completely in order to refocus or target the camera on that particular activity.

2.5 However, on occasions it can be useful to use this equipment to detect or prevent crime by means of a planned operation to record the activities of known or unknown persons. A comprehensive corporate guidance document exists to clearly define the processes and procedures that must be followed if such use is to be contemplated.

2.6 In these instances, CCTV operatives must not carry out targeted, planned surveillance which falls within RIPA without an appropriate authorisation.

2.7 It is not the responsibility of the CCTV operative to obtain such authorisation, which must always be in existence prior to any such activity commencing. Any individual approaching a CCTV operative without such an authorisation should be referred to the Senior Responsible Officer and be advised that any unauthorised use of the CCTV system would be unlawful and may give rise to a claim against the authority.

2.8 On occasions, the Authority may be approached by an outside law enforcement agency to help in their enquiry by utilising the Authority's CCTV equipment to undertake planned covert surveillance. Any approach of this nature must be referred to the Senior Responsible Officer and no such usage should ever be approved unless the agency concerned produces a valid RIPA authorisation.

APPENDIX 3

‘ACCESS’ AUTHORISATION APPLICATION FOR SOCIAL MEDIA

Referred to in Section F of the Corporate Guidance. To be adapted for each Service as applicable.

Contact: [Title] [First Name] [Surname]
Telephone: **[**Phone]
E-mail: [Email]
Web: www.durham/gov.uk
Case Ref: [CaseNo]

[ ] Team

To: [Name of Line Manager]
[Line Manager’s Job Title]

Date: [DATE]

REQUEST FOR SOCIAL MEDIA AUTHORISATION	
Customer Name	[Forename] [Surname]
Customer Address	[Address]
Names of person(s) or business(es) to be searched (list everyone/thing)	

Please give full details of what social media authorisation you require, with details of why this request will assist with the investigation, why you do not think privacy considerations are engaged and why you believe the Social Media site will hold this information:

[First Name] [Surname] [Job Title]

Manager's Decision			
Name		**Job Title**	
Signature		**Date**	
I am/am not* satisfied that accessing the social media account is appropriate and that a directed surveillance authorisation is/is not* required I authorise this request / I refuse this request * (* delete as appropriate)			
The password allocated to this request is: Remember you can only do an 'Open Source' check and only do one check for each account listed above. Any further monitoring will require a directed surveillance authorisation. This authorisation will expire in 10 working days. If the search is not completed within this time a new request will need to be completed. Please ensure you log out once you have completed your search and send a caller note to the [Relevant Service Officer] to inform them you have finished your search.			