www.erewash.gov.uk EREWASH BOROUGH COUNCIL

Regulation of Investigatory Powers Act 2000 (RIPA) Policy

Version: **Final**
Review Date: **April 2020**
Owner: **Head of Law and Corporate Governance**

CONTENTS

Page nos.

Appendices

Introduction

Erewash Borough Council only carries out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. It recognises its obligation to comply with RIPA when such an investigation is for the purpose of preventing or detecting crime or preventing disorder and has produced this guidance document to assist officers.

Applications for authority

An Authorising Officer will consider all applications for authorisation in accordance with RIPA. Any incomplete or inadequate application forms will be returned to the applicant for amendment. The authorising officer shall in particular ensure that:-

- there is a satisfactory reason for carrying out the surveillance
- the serious crime threshold is met
- the covert nature of the investigation is necessary
- proper consideration has been given to collateral intrusion
- the proposed length and extent of the surveillance is proportionate to the information being sought.
- Chief Executive's authorisation is sought where legal/medical/clerical issues are involved
- the authorisations are reviewed and cancelled.
- records of all authorisations are sent to the Borough Solicitor for entry on the Central Register.

A list of authorising officers is attached at Appendix A.

Once authorisation has been obtained from the authorising officer the investigating officer will attend the Magistrates' Court in order to obtain Judicial approval for the authorisation.

Training

Each Authorising Officer shall be responsible for ensuring that relevant members of staff are aware of the Act's requirements.

Central register and records.

The Head of Law and Corporate Governance shall retain the Central Register of all authorisations issued by Erewash Borough Council. The Head of Law and Corporate

Governance will also monitor the content of the application forms and authorisations to ensure that they comply with the Act.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

GUIDANCE - PART II

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

1 Purpose

The purpose of this guidance is to explain

the scope of RIPA – Part II

the circumstances where it applies, and

the authorisations procedures to be followed.

2 Introduction

2.1 This Act, which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and approved by the Judiciary before they are carried out.

2.2 The investigatory powers, which are relevant to a local authority, are directed covert surveillance in respect of specific operations involving 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 and tobacco, and the use of covert human intelligence sources. The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There is also a Code of Practice in relation to the use of these powers and this is attached at **Appendix D**.

2.3 Consideration must be given, prior to authorisation, as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be gleaned in other ways.

3 Scrutiny and Tribunal

3.1 External

3.1.1 As of 1 November 2012 the council has to obtain an order from a Justice of the Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity carried out.

3.1.2 The Office of Surveillance Commissioners (OSC) was set up to monitor compliance with RIPA. The Investigatory Powers Commissioner's Office took over the OSC's inspection and oversight responsibilities on 1 September 2017, and the Commissioner will from time to time inspect the council's records and procedures for this purpose.

3.1.3 In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. Applications will be heard on a judicial review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

3.1.4 The Tribunal can order:

- quashing or cancellation of any warrant or authorisation;
- destruction of any records or information obtained by using a warrant or authorisation; and
- destruction of records or information held by a public authority in relation to any person.

The council has a duty to disclose to the tribunal all documents they require if any council officer has:

- Granted any authorisation under RIPA
- Engaged in any conduct as a result of such authorisation

3.2 Internal

3.2.1 RIPA Monitoring Officer

The Head of Law and Corporate Governance is the Council's RIPA Monitoring Officer responsible for:

- Maintaining the Central Record of Authorisations
- Collating the original applications/authorisations, reviews, renewals and cancellations;
- Oversight of submitted RIPA documentation
- Organising a RIPA training programme; and
- Raising RIPA awareness within the council.

3.2.2 Senior Responsible Officer

The Head of Law and Corporate Governance is the Senior Responsible Officer responsible for:

- The integrity of the process in place within the council to authorise directed surveillance and CHIS
- Compliance with Part II of the 2000 Act and with accompanying Codes of Practice
- Engagement with the Commissioners and Inspectors when they conduct their inspections; and

- where necessary oversee the implementation of any post inspection action plans recommended or approved by a Commissioner.

Any officer considering using the RIPA provisions is invited to consult the Head of Law and Corporate Governance for advice at the earliest opportunity.

3.2.3 Elected Members

The elected members of the council will review the council's use of the 2000 Act and the authority's policy and guidance documents at least once a year. They will also consider internal reports on the use of the 2000 Act on 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 will not, however, be involved in making decisions on specific authorisations.

4 Benefits of RIPA authorisations

The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, RIPA provides a statutory framework under which covert surveillance can be authorised and conducted compatibly with Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings.

Section 78 Police and Criminal Evidence Act 1984 allows for the exclusion of evidence if it appears to the court that, having regard to all the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse affect on the fairness of the proceedings that the court ought not to admit it. Evidence obtained through covert surveillance will not be excluded unless the test of unfairness is met

5 Definitions

5.1 'Covert' is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place. (s.26 (9)(a))

5.2 'Covert human intelligence source' – put simply, this means the use of "agents, informants and officers working undercover", undercover officers or professional witnesses used to obtain information and evidence.

5.3 'Directed surveillance' is defined as covert but not intrusive and undertaken:

- for a specific investigation or operations;
- in such a way that is likely to result in the obtaining of private information about any person; and
- other than by way of an immediate response.(s.26 (2))

5.4 'Private information' is any information relating to a person in relation to which that person may or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.

5.5 'Intrusive' surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or using a surveillance device. **Erewash Borough Council may not authorise such surveillance**.

5.6 'Authorised officer' in the case of local authorities these are specified as Directors, Heads of Service, Service Managers or equivalent, responsible for the management of an investigation.

6 When does RIPA apply?

6.1 Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary for the purpose of preventing or detecting crime or of preventing disorder.

6.2 The council can only authorise directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or be an offence under:

a. S146 of the Licensing Act 2003 (sale of alcohol to children);

b. S147 of the Licensing Act 2003 (allowing the sale of alcohol to children);

c. S147A of the Licensing Act 2003 (persistently selling alcohol to children); and

d. S7 of the Children and Young Persons Act 1933 (sale of tobacco etc to persons under the age of 18)

6.3 CCTV

The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV to target a specific individual or group of individuals. Equally a request, say by the police, to track particular individuals via CCTV recordings may require authorisation (from the police).

6.4 Social Networking Sites

"The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation.

6.4.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of

privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

6.4.2 If it is necessary and proportionate for a public authority to breach covertly access controls the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

6.4.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

6.4.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done." (OSC guidance December 2014 paragraph 288).

6.4.5 When viewing social networking sites officers of a public authority should not use their personal equipment as it may be possible for the subject of interest or others to trace the officer's identity.

7 Covert Human Intelligence Source (CHIS)

7.1 Put simply, this means the use of "agents, informants and officers working undercover", undercover officers or professional witnesses used to obtain information and evidence.

7.2 The RIPA definition (section 26(8)) is anyone who:

a. establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b or c

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

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

Any reference to the conduct of a CHIS includes the conduct of a source which falls within a.to c. or is incidental to it.

References to the use of a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

7.3 Section 26(9) of RIPA goes on to define:-

a. a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and

b. a relationship is used covertly, and information obtained as mentioned in section 26(8)(c) above and is disclosed covertly, if, and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

7.4 There is a risk that an informant who is providing information to the council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised in the 2000 Act, not whether or not the CHIS is asked to do so by the council. When an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on any information from such an informant.

Urgent advice should be sought from the Head of Law and Corporate Governance should the use of CHIS be under consideration.

7.5 **Juvenile Sources**

Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility for him. The duration of a juvenile CHIS is one month. The Regulation of Investigatory Powers (Juveniles) Order 2000 SI No. 2793 contains special provisions which must be adhered to in respect of juvenile sources.

7.6 **Vulnerable Individuals**

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances.

8 Authorisations (see flowchart at appendix B)

8.1 Applications for directed surveillance

8.1.1 All application forms (**see appendix C**) must be fully completed with the required details to enable the authorising officer to make an informed decision.

No authorisation shall be granted unless the authorising officer is satisfied that the investigation is:

- necessary for either the purpose of preventing or detecting crime or of preventing disorder;
- involves a criminal offence punishable, whether summarily or on indictment, by a maximum sentence of at least 6 months imprisonment or relates to the underage sale of alcohol or tobacco;
- proportionate to the ultimate objective;
- at an appropriate level (i.e. not excessive); and
- that no other form of investigation would be appropriate.

The grant of authorisation should indicate that consideration has been given to the above points.

8.1.2 **Necessity and Proportionality:**

Obtaining an authorisation under the 2000 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

Necessity

The 2000 Act first requires that the person granting an authorisation believes that the authorisation is necessary in the circumstances of the particular case for the purpose of preventing or detecting crime or of preventing disorder.

Having considered whether there are grounds on which to authorise directed surveillance the authorising officer must also consider why it is necessary to conduct covert surveillance in the circumstances of the case.

Proportionality

Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

8.1.3 The authorising officer must also take into account the risk of **'collateral intrusion'** i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation, particularly where there are special sensitivities e.g. premises used by lawyers, doctors or priests e.g. for any form of medical or professional counselling or therapy. The application must include an assessment of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion.

Those carrying out the investigation must inform the authorising officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent.

8.1.4 **Special consideration in respect of confidential information**

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved.

Confidential information consists of personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Head of Law and Corporate Governance should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act.

Where such information is likely to be acquired, the surveillance may only be authorised by the Council's Head of Paid Service or, in his absence, the person acting as the Head of Paid Service.

8.1.5 **Notifications to Inspector/Commissioner**

The following situations must be brought to the Inspector/ Commissioner's attention at the next inspection:

- where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved;
- where a lawyer is the subject of an investigation or operation;
- where confidential personal information or confidential journalistic information has been acquired and retained.

8.1.6 **Applications for Covert Human Intelligence Source (CHIS)**

These are the same as for directed surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least six months imprisonment does not apply. The authorisation must specify the activities and identity (by pseudonym only) of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

8.1.7 **Judicial Approval of Authorisations**

Once the authorising officer has authorised the directed surveillance or CHIS, the authorising officer should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The authorising officer will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition the authorising officer will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the authorising officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate.

The Justice of the Peace will also consider whether there continues to be reasonable grounds.

The Justice of the Peace must also be satisfied that the person who granted the authorisation was an appropriate designated person and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for directed surveillance has been met.

The Justice of the Peace will record his/her decision on the order section of the judicial application/order form.

A copy of the RIPA form and judicial application/order form will be retained by the Court.

If the authorisation is approved the council may commence the activity.

If the Justice of the Peace refuses to approve the authorisation the council may not commence the activity although, if the reason for refusal is a technical error, the council may address this and reapply without going through the internal authorisation process again.

The Justice of the Peace may refuse to approve the authorisation, and quash it. The exercise of this power should not take place until the applicant has at least two business days from the date of the refusal to make representations.

9 Duration and Cancellation

- An authorisation for **directed surveillance** must be cancelled (if not renewed) within three months from the date of grant or renewal.

- An authorisation for **CHIS** must be cancelled (unless renewed) within 12 months from the date of grant or renewal.

This does not mean that the authorisation should be given for the whole period so that it lapses at the end of this time. The authorising officer, in accordance with s.45 of the Act, must cancel each authorisation as soon as that officer decides that the surveillance should be discontinued. Authorisations should only be operative for the minimum period reasonable for the purpose they are given.

On cancellation the cancellation form should detail what product has been obtained as a result of the surveillance activity. The form should include the dates and time of the activity, the nature of the product obtained and its format, any associated log or reference numbers, details of where the product is to be held and the name of the officer responsible for its future management.

10 Reviews

The authorising officer should review all authorisations at intervals determined by him/herself. This should be as often as necessary and practicable. The reviews should be recorded.

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals. It would be appropriate to call a review specifically for this purpose.

Particular attention should be paid to the possibility of obtaining confidential information.

11 Renewals

Any authorised officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect.

The renewal must then be approved by a Justice of the Peace in the same way as the original authorisation was approved.

The process outlined in paragraph 8.1.8 should be followed for reviews.

A CHIS authorisation must be thoroughly reviewed before it is renewed.

12 Central Record of authorisations

Originals of all forms must be submitted to the Head of Law and Corporate Governance as soon as they are completed for inclusion in the Central Record of authorisations.

Directed surveillance

12.1 A centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Commissioner or Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for up to a period of at least three years from the ending of the authorisation and should contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- the date the approval order was given by the Justice of the Peace;
- the name and grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of investigation or operation, including a brief description on names of subjects, if known;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and grade of the authorising officer;
- the dates of any approval order for renewal given by the Justice of the Peace;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in the covert surveillance code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation; and
- the date the authorisation was cancelled.

12.2 In all cases the authority should maintain the following documentation which need not form part of the centrally retrievable record:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of any authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when the instruction to cease surveillance was given;
- the date and time when any other instruction was given by the authorising officer;

12.3 **Covert Human Intelligence Source (CHIS)**

A centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever authorisation is granted, renewed or cancelled. The record should be made available to the relevant Commissioner or Inspector from the Investigatory Powers Commissioner's Office upon request. These records should be retained for a period of at least three years from the ending of the authorisation.

12.4 Proper records must be kept of the authorisation and the use of the source. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with a responsibility for maintaining a record of the use made of the source. The regulation of Investigatory Powers (Source Records) Regulations 2000; SI.2725 details the particulars that must be included in the records relating to each source.

12.5 In addition records or copies of the following, as appropriate, should be kept by the relevant authority:

- a copy of the authorisation together with any supplementary authorisation and notification of approval given by the authorising officer;
- a copy of any renewal of any authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing the authorisation considered it necessary to do so;
- any risk assessment made in relation to the source;
- the circumstances in which the tasks were given to the source;
- the values of the source to the investigation authority;
- a record of the result of any reviews of the authorisation;
- the reason, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation; and

- the date and time when any instruction was given by the authorising officer to cease using the source.

12.6 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. The Head of Law and Corporate Governance will have responsibility for maintaining a record of the use made of the source.

13 Retention of records

All documents must be treated as strictly confidential and the authorising officer must make appropriate arrangements for their retention, security and destruction, in accordance with the council's Data Protection Policy and the RIPA codes of practice. The retention period for the purposes of this guidance is three years from the ending of the period authorised.

14 Complaints procedure

14.1 The council will maintain the standards set out in this guidance and the Codes of Practice (**See Appendix D**). The Investigatory Powers Commissioner's Office has responsibility for monitoring and reviewing the way the council exercises the powers and duties conferred by RIPA.

14.2 Contravention of the Data Protection Act 1998 may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this guidance should be made using the council's own internal complaints procedure. To request a complaints form, please contact the *Monitoring Officer, Town Hall, Ilkeston, Derbyshire, DE7 5RP or telephone 0115 907 1132.*

14.3 The 2000 Act establishes an Independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal, PO BOX 33220, London SWLH 9ZQ
Telephone 020 7035 3711

REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDANCE – CHAPTER II OF PART I

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Introduction

With effect from 5 January 2004, and in accordance with Part I of Chapter I of Regulation of Investigatory Powers Act ('the Act'), local authorities can authorise the acquisition and disclosure of 'communications data' provided that the acquisition of such data is necessary for the purpose of **preventing or detecting crime or preventing disorder**; and proportionate to what is sought to be achieved by acquiring such data.

There is a Code of Practice **(Appendix F**) ('the code').

NOTHING IN THIS CODE PERMITS THE INTERCEPTION OF THE CONTENT OF ANY COMMUNICATION.

The procedure is similar to that of authorisation for directed surveillance and CHIS but has extra provisions and processes.

The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge.

The authorising officer is called a 'designated person'.

1. What is 'Communications data'?

Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories:-

Traffic data – where a communication was made from, to whom and when

Service data – use made of service e.g. itemised telephone records

Subscriber data – information held or obtained by operator on person they provide a service to.

Local authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

2. Designated person

A designated person must be at least the level of Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent.

3. Application forms

All applications must be made on a standard form (**Appendix G)** and submitted to the Single Point of Contact (SPOC). The SPOC will ensure that the application meets the required criteria and then pass to the Designated Person.

4. Authorisations

Authorisations can only authorise conduct to which Chapter II of Part I of the Act applies.

In order to comply with the code, a designated person can only authorise the obtaining and disclosure of communications data if:

i) It is **necessary** for any of the purposes set out in Section 22(2) of the Act. (NB Erewash Borough Council can only authorise for the purpose set out in Section 22 (2) (b) which is the purpose of preventing or detecting crime or preventing disorder); and

ii) It is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act)

Consideration must also be given to the possibility of collateral intrusion and whether any urgent timescale is justified.

Once a designated person has decided to grant an authorisation or a notice given there are two methods: -

1) By authorisation of some person in the same relevant public authority as the designated person, whereby the relevant public authority collects the data itself (Section 22(3) the Act). This may be appropriate in the following circumstances:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

2) By notice to the holder of the data to be acquired (Section 22(4)) which requires the operator to collect or retrieve the data. Disclosure may only be required to either the designated person or the single point of contact.

   Service provider must comply with the notice if it is reasonably practicable to do so (s.22 (6)-(8)) and can be enforced to do so by civil proceedings.

   The postal or telecommunications service can charge for providing this information.

   There are standard forms (**Appendix H**) for authorisations and notice.

5. Oral authority

Erewash Borough Council is not permitted to apply or approve orally.

6. Single point of contact (SPOC)

Notices and authorisations should be passed through a single point of contact within the council. This should make the system operate more efficiently as the SPOC will deal with the postal or telecommunications operator on a regular basis and also be in a position to advise a designated person on the appropriateness of an authorisation or notice.

SPOCs should be in position to:

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated person on whether communications data falls under section 21(4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

A SPOC must be accredited which involves undertaking appropriate training.

7. Duration

Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

8. Renewal and cancellation

An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

The code requires that all authorisations and notices should be cancelled by the designated person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant postal or telecommunications operator should be informed of the cancellation of a notice.

9. Retention of records

Applications, authorisations and notices must be retained until the council has been audited by the Commissioner (see paragraph 10).

Applications must also be retained to allow the Tribunal (see paragraph 10) to carry out its functions.

A record must be kept of:

- the dates on which the authorisation or notice is started or cancelled.

- any errors that have occurred in the granting of authorisations or giving of notices.

A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable.

Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 1998 must be observed.

The Head of Law and Corporate Governance will maintain a centrally retrievable register.

10. Oversight and Complaints

The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained in Part I and the code requires any person who uses the powers conferred by Chapter II to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions. From 1 September 2017 this function has been transferred to the Investigatory Powers Commissioner's Office.

The Act also establishes an independent Tribunal to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure should be available for reference at Erewash Borough Council's public offices.

APPENDIX A

EREWASH BOROUGH COUNCIL'S AUTHORISING OFFICERS

Chief Executive – Jeremy Jaroszek

Director of Resources and Deputy Chief Executive – Ian Sankey

Exchequer Services Manager – John Drewett

Internal Audit Manager – Andy Hill

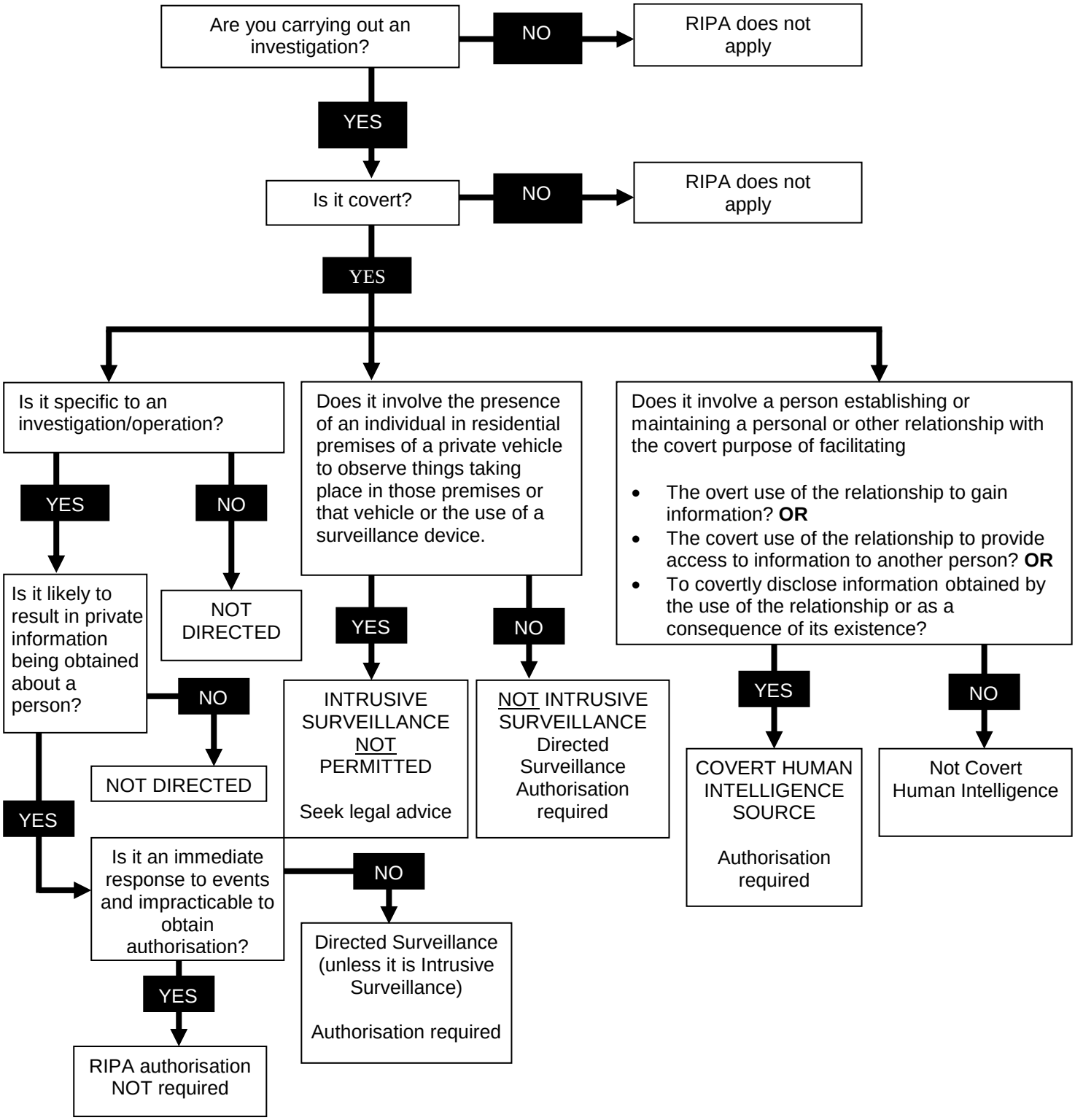
Head of Environment and Housing Services – Nick Thurstan

APPENDIX B

DIRECTED SURVEILLANCE FLOWCHART

Regulation of Investigatory Powers Act 2000

Do you need Authorisation?



APPENDIX C

Application Forms

Directed Surveillance and Covert Human Intelligence Source (CHIS) Forms

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-directed-surveillance?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan?view=Binary

Judicial Approval

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/approval-order-form?view=Binary

APPENDIX C

Forms

Directed Surveillance and Covert Human Intelligence Source (CHIS) Forms

APPLICATION

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application?view=Binary

REVIEW

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review?view=Binary

RENEWAL

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal?view=Binary

CANCELLATION

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation?view=Binary

APPENDIX D

Code of Practice

Covert Surveillance and Property Interference and Covert Human Intelligence Source (CHIS) Codes of Practice

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary

Code of Practice

Covert Human Intelligence Sources (CHIS)

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-human-intel?view=Binary

Procedures and Guidance

See Office of Surveillance Commissioners website:

https://osc.independent.gov.uk

APPENDIX E

Protection of Freedom Act 2012 – Changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary

APPENDIX F

Code of Practice

Acquisition and Disclosure of Communications Data

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary

APPENDIX G

Application Form for Communications Data

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/communications-data1.doc?view=Binary

APPENDIX H

Notice

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/ripa-section-22-notice-update?view=Binary

Accredited SPoC Notifying IOCCO of a Reportable Error

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/reporting-public-authority-error?view=Binary