South Staffordshire Council

Corporate Policy and Guidance Document on on the Regulation of Investigatory Powers Act 2000 (RIPA)

www.sstaffs.gov.uk

The Regulation of Investigatory Powers Act 2000 (RIPA)

CONTENTS

NB:

The Regulation of Investigatory Powers Act 2000 ('RIPA') ("the Act") refers to 'Designated Officers'. For ease of understanding and application within South Staffordshire Council, this Corporate Policy & Guidance Document refers to 'Authorising Officers'. For the avoidance of doubt, therefore, all references to 'Authorising Officers' refer to 'designated officers' as described in the Act.

Version Date: V.10
Review Date: October 2023

A. INTRODUCTION AND KEY MESSAGE

1. South Staffordshire Council is fully committed to operating its covert investigation activities in the letter and the spirit of the Regulation of Investigatory Powers Act 2000 (RIPA) as it provides protection for the legitimate rights of people living or working or visiting the District. Whilst fully supporting these fundamental rights South Staffordshire Council will deliver effective enforcement services that protect the wider public interest by the necessary and proportionate use of lawful covert investigation techniques.

   South Staffordshire Council takes its responsibilities under RIPA for ensuring that any actions authorised in possession of its RIPA powers are both necessary and proportionate, extremely seriously. To this end the council has approved this Policy and Guidance Document, which will be kept under review as to its effectiveness and appropriateness by the Corporate Director of Governance.

2. The Human Rights Act 1998 (which brought much of the European Convention for the Protection of Human Rights and Fundamental Freedoms into UK domestic law) requires the council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and their correspondence.

3. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the council may interfere in the citizen's right mentioned above, if such interference is:

   A. in accordance with the law;

   B. necessary (as defined in this document); and

   C. proportionate (as defined in this document).

4. RIPA provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance and the use of a 'covert human intelligence source' (CHIS) – e.g. undercover agents - or the acquisition of communications data (as defined later in this document). It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

5. The purpose of this guidance is to:

   - explain the scope of RIPA and the circumstances where it applies
   - provide guidance on the authorisation procedures to be followed

6. The council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance. If any doubt arises, the Home Office Code of Practice should be consulted; the Code of Practice takes precedence over this guidance.

   Covert Human Intelligence Sources

   Covert Surveillance

   Communications Data

   The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. Staff should refer to the Home Office Codes of Practice for supplementary guidance.

   In addition, further guidance in respect of the judicial approval process and the crime threshold has been issued by the Home Office:

   RIPA Guidance

   This is non-statutory guidance but should be consulted as necessary.

7. Directly employed council staff and external agencies working for the council are covered by the Act for the time they are working for the council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the council's behalf must be properly authorised by one of the council's designated Authorising Officers.

8. If the correct procedures are not followed, evidence obtained through the use of covert surveillance, a CHIS or the acquisition of communications data, may be disallowed by the courts, resulting in the possible loss of what would otherwise have been a successful prosecution and the potential for costs to be awarded against the council or even an individual officer. In addition, a complaint of maladministration could be made to the Ombudsman, and the council could be ordered to pay compensation. Furthermore, any individual who is aggrieved by any act by the council or any of its staff may seek damages through the courts. Such action would not, of course, promote the good reputation of the council and could be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Corporate Director of Governance.

9. A flowchart of the procedures to be followed appears at **Appendix 2**.

10. The authoritative position on RIPA is, of course, the Act itself and any officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Corporate Director of Governance for advice and assistance. Appropriate training and development will be organised and training given to Authorising Officers and Applicants and any other Senior Manager who may from time to time need to seek authorisation under RIPA.

11. The Corporate Director of Governance will maintain and check the corporate register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to ensure the Corporate Director of Governance receives a copy of the relevant forms as soon as possible but in any event within five working days of authorisation, review, renewal, cancellation or rejection.

12. RIPA and this document are important for the effective and efficient operation of the council's actions with regard to the use of covert surveillance, CHIS and the acquisition and disclosure of communications data. Therefore, this document will be kept under annual review by Corporate Director of Governance. Authorising officers and applicants should bring any suggestions for continuous improvement of this document to the attention of the Corporate Director of Governance at the earliest possible opportunity.

13. In terms of monitoring e-mails and internet usage, it is important to recognise the important relationship and overlap with the council's current e-mail and internet policies and guidance; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, and the Data Protection Act 2018. RIPA forms should only be used wherever relevant and are only relevant where the criteria listed on the forms are fully met. Under normal circumstances the council's E-mail and Internet Usage Policies should be used, as any surveillance is likely to be more relevant under terms of employment as opposed to RIPA.

14. Confidential personal information (information where a high degree of privacy may be expected due to the relationship between the parties concerned e.g. solicitor/client; priest/parishioner; journalist/informant; counsellor/consultee, etc) will not be acquired as a result of any covert surveillance, the use of CHIS and the acquisition and disclosure of communications employed by the council. Where there is any identified risk of acquiring confidential information prior to authorisation, then such activity shall only be authorised by the Chief Executive.

15. The acquisition of communications data shall be undertaken through a Clearing House, thus avoiding the need for the council to employ a Single Point of Contact (SPOC) under RIPA (and associated legislation) and the Home Office Code of Practice.

16. RIPA states that:

"if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be "lawful for all purposes".

However, the opposite is not true - i.e. if you do not obtain RIPA authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits and you may have to justify infringing a person's Human Rights and any evidence you place before the courts may be subject to challenge in respect of the processes used to obtain the evidence (s78 Police and Criminal Evidence Act 1984).

17. If you are in any doubt with regard to the RIPA, this document or the related legislative provisions, please consult the Corporate Director of Governance at the earliest possible opportunity.

B. COUNCIL POLICY STATEMENT

1. The council takes its statutory responsibilities seriously and will, at all times, act in accordance with the law and take necessary and proportionate action in this regard. The Corporate Director of Governance is duly authorised by the council to keep this document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administration and operational effectiveness, the Corporate Director of Governance is also authorised to add or substitute officers authorised for the purpose of RIPA in consultation with the Chief Executive.

2. The council has adopted a policy to the effect:

   a. that applicable covert surveillance operations, the use of CHIS and the acquisition and disclosure of communications data conducted by the council should comply with the requirements of RIPA and the Home Office Codes of Practice;
   b. that only the officers detailed in **Appendix 1** shall be permitted to authorise a covert surveillance exercise, a CHIS or the acquisition of communications data, subject in each case to the restrictions noted in that appendix.
   c. that, where it is judged necessary to obtain it, the acquisition of communications data shall be undertaken through a Clearing House, thus avoiding the need for the council to employ a Single Point of Contact (SPOC) under RIPA (and associated legislation) and the Home Office Code of Practice;

d. that covert surveillance; CHIS and the acquisition and disclosure of communications data shall only be employed when necessary for the purposes of the prevention or detection of crime or preventing disorder and when such action is considered to be proportionate to the offence or disorder concerned; and
e. that this document and the Home Office Codes of Practice be brought to the attention of all the staff who may carry out covert surveillance or the use of CHIS.

3. Operations under RIPA can be authorised only on the following ground:

- **For the purpose of preventing or detecting crime or of preventing disorder.**

In order for a directed surveillance authorisation to be made, the serious crime test must be passed. This means there must be a criminal offence and the offence under investigation must carry a sentence of six months imprisonment. There is an exception for underage sale operations in respect of alcohol and tobacco sales.

4. In assessing whether or not the proposed surveillance is necessary and proportionate, the authorising officer must consider other appropriate means of gathering the information. The least intrusive method will be considered proportionate by the Courts. Surveillance activity should only be used as a last resort.

HRA Assessments outside of RIPA

5. The council may wish to undertake surveillance (e.g. noise monitoring prior to service of an Abatement Notice or use of CCTV cameras for fly-tipping operations) and may on occasion determine that this should be on a covert basis. As detailed in this document, noise monitoring is usually notified to the person being monitored and therefore is outside of RIPA. However, if in particular circumstances, covert surveillance is considered appropriate outside of RIPA, then a full HRA assessment should be undertaken. The same forms as for RIPA should be used, as HRA Assessment Forms, and be authorised in the usual way (there is no need for Judicial Approval). This will assist in considering and assessing the issues and also protecting the council if challenged under HRA.

C. AUTHORISING OFFICER RESPONSIBILITES

1. The policy and guidance in this document will become operative with effect from October 2023. It is essential, therefore, that applicants take personal responsibility for the effective and efficient operation of this document.

2. Certain officers have delegated power to authorise applications under RIPA, always provided that the officer is sufficiently removed from the investigation that they can be deemed to manage it but are not involved in its day to day conduct (i.e.: they MUST NOT take part in the surveillance or in the management of the Covert Human Intelligence Source to which the application relates). This will usually allow a delegation down to a level such as Assistant Director.

3. It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.

4. Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Guidance Document and do not undertake or carry out any form of covert surveillance without first obtaining the relevant authorisations in compliance with this Document.

5. The Corporate Leadership Team will also ensure that staff who report to them follow this policy and guidance document and do not undertake or carry out any form of surveillance or seek the acquisition of communications data without first obtaining the relevant authorisations in compliance with this document.

6. Authorising Officers must also pay particular attention to health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an authorising officer approve any RIPA form unless, and until they are satisfied the health and safety of council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an authorising officer is in any doubt, they should obtain prior guidance on the same from their Director, the Health & Safety Officer and/or the Corporate Director of Governance.

7. Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA. Any failure to comply exposes the council to unnecessary legal risks and criticism from the Investigatory Powers Commissioner's Office (IPCO). Cancellations must be dealt with promptly.

9. Inadvertently obtaining confidential information during surveillance must be given prior thought before any application, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a RIPA Authorisation. Where there is any possibility of confidential information being obtained through covert surveillance, the application must be authorised by the Chief Executive.

10. Authorising officers must ensure proper regard is had to necessity and proportionality before any applications are authorised. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail had been given to the particular circumstances of any person likely to be the subject of the authorisation. Any equipment to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

11. Authorising Officers must also ensure that, when sending copies of any forms to the Corporate Director of Governance (or any other relevant authority), they are sent in sealed envelopes and marked 'Private & Confidential'.

12. Authorising Officers must also address the issue of what will happen to the product of the surveillance (i.e. the evidence obtained) and this must be detailed on the form. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

    There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

D. WHAT RIPA DOES AND DOES NOT DO

1. RIPA **does**:

   - require prior authorisation of directed surveillance;
   - require prior authorisation of the conduct and use of a CHIS;
   - require prior authorisation for the acquisition of communications data;
   - require safeguards for the conduct and use of a CHIS;
   - limit the purposes for which covert surveillance, CHIS or the acquisition of communications data may be used by the council, and
   - prohibit the council from carrying out intrusive surveillance.

2. RIPA **does not**:
   - make lawful conduct which is otherwise unlawful, or
   - prejudice or dis-apply any existing powers available to the council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

3. If an Authorising Officer or any applicant is in any doubt, they should seek advice from the Corporate Director of Governance before any directed surveillance or CHIS is authorised, renewed, cancelled or rejected, or any acquisition of communications data sought.

E. TYPES OF SURVEILLANCE

1. 'Surveillance' includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- recording anything mentioned above in the course of authorised surveillance.
- surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

2. Overt Surveillance

Most of the surveillance carried out by the council will be done overtly - there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where a premises licence is issued subject to conditions, and the licence holder is told that officers may visit without notice or identifying themselves to the owner/ proprietor to check that the conditions are being met.

3. Covert Surveillance

Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA).

RIPA regulates three types of covert surveillance: directed surveillance; intrusive surveillance and the use of covert human intelligence sources (CHIS).

4. Directed Surveillance

Directed Surveillance is surveillance which:

- is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information (see definition below) about an individual (whether or not that person is specifically targeted for purposes of an investigation) (Section 26(10) of RIPA) and
- is covert; and
- is not intrusive surveillance (see definition below – the council must not carry out any intrusive surveillance); and
- is not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it for a short time.

5. Private Information

Private information in relation to a person includes any information relating to their private and family life, their home and their correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. The definition of private information has been given a wide interpretation by the Courts and will include business information in appropriate circumstances. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about them and possibly others that they come into contact, or associate, with (collateral intrusion).

Following a review of operating procedures, the council will no longer seek RIPA authorisation for covert use of CCTV cameras in respect of fly-tipping operations. This is on the basis that such operations are unlikely to include the obtaining of private information as defined. Such operations will be subject to a HRA assessment but generally will not require RIPA authorisation.

Similarly, although overt public realm CCTV cameras do not normally require authorisation; if the camera is tasked for a specific purpose which involves the prolonged surveillance of a particular person or persons, authorisation will be required. The way a person runs their business may also reveal information about his or her private life and the private lives of others.

The use of CCTV in South Staffordshire is subject to its own Policy, Procedure and Protocols as developed by the council. The CCTV policy is viewed as complementary to this policy document.

For the avoidance of doubt, only those officers designated and certified as Authorising Officers for the purpose of RIPA can authorise 'directed surveillance' if and only if the RIPA authorisation procedures detailed in this Document are followed. If an Authorising Officer has not been 'certified' for the purposes of RIPA, she/he can NOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

6. Intrusive Surveillance

This is when the surveillance is:

- covert;
- relates to residential premises or private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if it were in the premises/vehicle. Merely observing movements from/to a house from a parked vehicle will not be classed as intrusive surveillance.

This form of surveillance can be carried out only by Police and other law enforcement agencies. Council officers must not carry out intrusive surveillance. Likewise, the council has no statutory powers to interfere with private property

7. Employee Surveillance using Covert Surveillance

Following a decision of the Surveillance Tribunal, it has been established that RIPA authorisation is not required where the surveillance is undertaken as part of an investigation in relation to an employee's misconduct or breach of the terms and conditions of the employee's contract of employment i.e. any investigation undertaken other than into an alleged criminal offence.

However, such surveillance may still potentially be viewed as infringing the employee's right to privacy as established under Article 8 of the Human Rights Act.

Where such surveillance, pertaining to a non-criminal investigation into the conduct of an employee is required, officers are required to complete the appropriate form, as for RIPA, and then forward the form to a Senior Authorising Officer for approval. The applicant is not required to be one of the employees listed in **Appendix 1**.

For purposes of consistency, authorisations will last for three months and appropriate action must be taken to review, renew and cancel authorisations.

The Senior Authorising Officer will apply the same criteria as if the request was for RIPA authorisation.

Once authorised, a signed copy of the authorised form and subsequent review, renewal and cancellation forms must be kept secure with the investigation file. **There is no requirement to log the authorisation on the Central Register.**

8. Social Networks

The use of the internet and in particular social networking sites is increasingly an area used by Investigating Officers. The following extract from the previously issued OSC Guidance should be considered before any such use:

Covert surveillance of Social Networking Sites (SNS)

The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

- 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.

- Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, 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).

- 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 for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

- 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).

Officers are also required to be aware of and take account of the Home Office Guidance in particular paragraphs 3.10 – 3.17 and 4.11 – 4.16.

Officers should consult with the Corporate Director of Governance before using social media for any covert/investigatory purpose. It is imperative that the council does not inadvertently undertake unauthorised surveillance in this area. In particular, officers should be aware that anything more than an initial check on a person MAY require authorisation. Officers must check before proceeding.

9. Proportionality

The term contains three concepts:

- the means should not be excessive by relation to the gravity of the crime or disorder being investigated.
- the least intrusive means of surveillance.
- collateral intrusion involves invasion of third parties' privacy and should, so far as is possible be minimised.

In other words, this involves balancing the intrusiveness of the activity on the subject 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 – each case will be judged and be unique on its merits - or if the information which is sought could be reasonably obtained by other less intrusive means. All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Extra care should also be taken over any publication of the product of the surveillance.

10. Examples of different types of surveillance

Type of surveillance	Examples
Overt	» Police officer or parks warden on patrol. » Signposted town centre CCTV cameras (in normal use). » Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. » Sampling purchases (where the officer behaves no differently from a normal member of the public). » Dog warden in uniform on patrol in park, street or van » Food safety or health & safety inspections.
Covert but not requiring prior authorisation	» CCTV cameras providing general traffic, crime or public safety information.
Directed must be RIPA authorised.	» Officers follow an individual or individuals over a period, to establish whether they are working when claiming benefit or has long term sick leave from employment. » Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where they are suspected of running their business in an unlawful manner. » Surveillance of a property in relation to the movement or selling of illegal food products.
Intrusive - **the council cannot do this.**	» Planting a listening or other device in a person's home or in their private vehicle.
Interception of telecommunication apparatus - **the council cannot do this.**	» Phone tapping etc.

11. Further Information

Further guidance on surveillance can be found in the Home Office Code of Practice on surveillance. A database has been established on "The Core" giving further reference documents regarding RIPA authorisations; including the Home Office Codes of Practice.

12. Confidential Information

Special safeguards apply with regard to confidential information relating to legal privilege, personal information and journalistic material. The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and cannot be obtained. Further guidance is available in the Home Office Codes of Practice.

13. Collateral Intrusion

Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

Those carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation.

Further guidance is available in the Home Office Codes of Practice.

14. Risk Assessment

A risk assessment must be undertaken for each application.

15. Retention and Destruction of Product of Surveillance

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

F. CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

1. Who is a CHIS?

- Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.
- 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 the purpose behind the relationship.
- RIPA does not apply in circumstances where members of the public volunteer information to the council as part of their normal civic duties, or to contact numbers set up to receive information.
- If information is received via hotline or similar, this does not constitute a CHIS.
- South Staffordshire Council guidance is not to ask the informant to gather information on the council's behalf, as this may result in forming a relationship with the subject and therefore becoming a CHIS.

2. What must be authorised?

The conduct or use of a CHIS requires prior authorisation.

Conduct of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information about another person or persons.

Use of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

3. Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). **Contact the Corporate Director of Governance if considering use of a juvenile source.**

4. 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 themselves or unable to protect themselves against significant harm or exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances. **Contact the Corporate Director of Governance if considering use of a vulnerable source.**

5. Test Purchases

Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS). Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

6. Anti-social behaviour activities (e.g. noise, violence, race etc)

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a Digital Audio Type recorder) on private premises could constitute intrusive surveillance unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation, unless the system complies with the CCTV statutory code of practice, and there is clear signage indicating the use of CCTV and the purposes for which the information may be used.

G. COMMUNICATIONS DATA

What is Communications Data?

1. Communications data means any traffic or any information that is or has been sent by or over a telecommunications system or postal system, together with information about the use of the system made by any person.

Procedure

2. There are two powers granted by s.22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Service Provider").
3. S.22(3) provides that any authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a Communications Service Provider is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves.
4. In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under s.22(4) RIPA must be issued. The sole grounds to permit the issuing of a s.22 notice by a Permitted Local Authority is for the purposes of **"preventing or detecting crime or of preventing disorder"**. The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Service Provider will most probably have means of collating and providing the communications data requested.
5. Use of s.22(3) should only be used where the local authority is seeking to collect the information themselves, i.e. either to install its own monitoring system or using its own staff to obtain the information from the Communications Service Provider.
6. Use of s.22(4) should be used when the Communications Service Provider is being required to disclose or obtain and disclose the specified information.

   The council uses the National Anti-Fraud Network (NAFN) to undertake the Single Point of Contact (SPoC) role in respect of communications data applications. NAFN should be contacted by the Applicant at any early stage in order to ensure the application is appropriate. An Authorising Officer will be notified by the SPoC at NAFN when an application is awaiting approval. NAFN will manage the process and hold records on behalf of the council.
7. Once a notice has been issued, it must be sent to the Communications Service Provider. In issuing a notice, the Authorising Officer can authorise another person to liaise with the Communications Service Provider covered by the notice. This function will be undertaken by NAFN.
8. For the council Authorising Officers who have been duly authorised by the Corporate Director of Governance for the purposes of RIPA may sign the Communications Data forms. Copies of forms must be provided to the Corporate Director of Governance within five working days signing.

H. AUTHORISATION PROCEDURES

Directed surveillance, the use of a CHIS and the acquisition of communications data can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides a flow chart of process from application consideration to recording of information.

1. Authorising Officers

Forms can only be signed by Authorising Officers who have attended appropriate training. Authorised posts are listed in **Appendix 1**. This appendix will be kept up to date by the Corporate Director of Governance, and added to as needs require. The Corporate Director of Governance has been duly authorised to add, delete or substitute posts listed in **Appendix 1** as approved by the Chief Executive.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal Schemes of Management. All RIPA authorisations, save for authorisations to collect communications data under s.22 (3), are for specific investigations only, they must be reviewed at a minimum at monthly intervals and must be renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time! Authorisations to collect communications data under s.22 (3) have a lifespan of one month. However, they can be renewed by serving a new authorisation or notice for further months, within any time within the current life of the notice. It is the personal responsibility of the Authorising Officer to ensure that dates are adhered to; it is not the responsibility of the applicant.

2. Training Records

Proper training will be given before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training will be kept by the Corporate Director of Governance.

If the Corporate Director of Governance feels that an Authorising Officer has not complied fully with the requirements of this document, or the training provided to them, the Corporate Director of Governance is duly authorised to retract that officer's authorisation until they have undertaken further approved training or one to one guidance from, or arranged by the Corporate Director of Governance.

3. Application Forms

Only the approved RIPA forms downloaded from the Home Office website must be used. Any other forms will be rejected by the authorising officer and/or the Corporate Director of Governance.

A plan indicating the area where surveillance is to take place together with proposed surveillance points should be included to enable the authorising officer to better assess the potential for collateral intrusion. A postcode for each property to be kept under surveillance should be included on all forms.

4. Grounds for Authorisation

Directed Surveillance or the Conduct and Use of the CHIS and/or disclosure of communications data can be authorised by the council only on the following ground:-

- For the prevention or detection of crime or of preventing disorder

No other grounds are available to local authorities.

In addition, for Directed Surveillance, the offence under investigation must be one that carries a sentence of six months imprisonment. There is an exception to this requirement in respect of test purchase operations for sales of age restricted products (alcohol and tobacco).

5. Assessing the Application Form

Before an Authorising Officer signs a form, they must:

(a) be mindful of the requirements policy & procedures document; the training provided by the council and any other guidance issued, from time to time, by the Corporate Director of Governance on such matters;

(b) satisfy themselves that the RIPA authorisation is:-

(i) in accordance with the law;
(ii) necessary in the circumstances of the particular case for the prevention or detection of crime or for preventing disorder; and
(iii) proportionate to what it seeks to achieve.

(c) in assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information. **The less intrusive method will be considered proportionate by the courts.** Furthermore, the level of surveillance must be proportionate to the offence or disorder under investigation or for which a prosecution is sought.

(d) take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining the level of proportionality;

(e) set a date for a review of the authorisation and ensure that a review takes place no later than that date;

(f) obtain a Unique Reference Number (URN) for the application as follows:

Year/Authorising Officer Code/Number of Application

(g) ensure that a copy of the RIPA forms (and any review/cancellation of the same) is forwarded to the Corporate Director of Governance for inclusion in the central register, **within five working days of the relevant authorisation, review, renewal, cancellation or rejection.**

6. Risk Assessment

Each application should be accompanied by a risk assessment proforma (R.A.1). An authorising officer may not approve an application for covert surveillance in the absence of such an assessment.

7. Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorising Officer must also:

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved;
(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;
(c) consider the likely degree of intrusion of all those potentially affected;
(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and
(e) ensure records contain particulars and are not available except on a need to know basis.

The requirements of s.29(5) RIPA and the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI: 2000/2725) must be considered and applied when authorising the use of a CHIS. Contact the Corporate Director of Governance for advice on the requirements if required.

8. Judicial Approval - all applications

Once an application has been approved by the Authorising Officer, the Applicant must contact Newcastle Magistrates' Court to obtain consent from a JP. The Applicant must attend the Court and provide the following to the Court:

- Application
- Supporting Information
- Draft Consent Order

NB: An application is not active until consent of a JP is obtained and no activity must occur prior to the consent of the JP being obtained.

9. Urgent Authorisations

As all applications have to be approved by a JP, urgent oral authorisations are not longer available.

10. Duration

The Authorisation **must be reviewed and renewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for three months (from authorisation) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, the Authorisations do not expire! The authorisations have to be reviewed, renewed and/or cancelled (once they are no longer required)!

Notices/Authorities issued under s.22 compelling disclosure of Communications Data are only valid for one month, but can be renewed for subsequent period of one month at any time.

Authorisations can be renewed in writing before the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

A renewal must also be approved by a JP in the same way as an original application.

I. WORKING WITH OR THROUGH OTHER AGENCIES

1. When some other agency has been instructed on behalf of the council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):

   (a) wishes to use the council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the council's resources to be used for the other agency's purposes, he/she must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Corporate Director of Governance for the central register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the council and the use of its resources;

   (b) wishes to use the council's premises for their own RIPA action, the council should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the council's co-operation in the agency's RIPA operation. In such cases the council's own RIPA forms should not be used as the council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

3. In terms of 2(a), if the police or other agency wishes to use council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any council resources are made available for the proposed use.

   A council Authorising Officer can grant a directed surveillance authorisation to cover both council and Government Department investigators involved in a joint investigation. Equally a Government Department Authorising Officer can do the same on a joint investigation.

   The nominated investigator from the organisation with primary responsibility will complete the application, including the names and organisation of all investigators likely to be involved in the surveillance. The Authorising Officer from the lead organisation must make the decision on suitability for surveillance to take place. The Authorising Officer must retain records as described in paragraphs J2 to J4 (Record Management).

To ensure that the Authorising Officer is aware of the full facts of the case, the applicant must record the following information on the RIPA form:

- That the request for surveillance is part of a joint investigation.
- Include how many of the officers to be deployed at any one time are investigators from the council or Government Department.
- If possible, name the investigators involved.

Where joint surveillance is authorised by one organisation (i.e. the lead organisation), it is good practice for the Investigating Officer/Manager of the other organisation to advise their Authorising Officer of the surveillance activity. This advice is given so that each authorising officer is aware of all surveillance activity being undertaken by their own investigators, regardless of which organisation authorised the activity.

If in doubt, please consult with the Corporate Director of Governance at the earliest opportunity.

J. RECORDS MANAGEMENT

The council must keep a detailed record of all authorisations, renewals, cancellations and rejections. A central register of all authorisation forms will be maintained and monitored by the Corporate Director of Governance.

1. Central Register maintained by the Corporate Director of Governance.

The following documents must be retained by the Corporate Director of Governance for such purposes.

The central register includes:

- the original completed RIPA, CHIS and COMMS forms together with any supplementary documentation and notification of the approval given by the authorising officer
- a record of the type of authorisation, date given and the name of authorising officer
- the title of the investigation and a description
- whether the urgency provisions have been utilised
- the frequency of reviews prescribed by the authorising officer
- that confidential information is not anticipated to be acquired
- the date cancelled
- the unique reference number for the authorisation (URN).

The council will retain the central records for a period of at least three years from the ending of the authorisation. The Investigatory Powers Commissioner's Office can audit/review the council's policies and procedures, and individual authorisations

Each form will have a URN which is issued at the time of the original authorisation and must be shown on all subsequent forms. The Corporate Director of Governance will issue the relevant URN to applicants.

Authorising Officers must forward originals of all completed forms to the Corporate Director of Governance for the central register, within five working days of the authorisation, review, renewal, cancellation or rejection. The Corporate Director of Governance will monitor the same and give appropriate guidance, from time to time, or amend this document, as necessary.

As part of the central record a control matrix will be maintained by the Corporate Director of Governance, to record the progress of each application.

2. Records which must be maintained in the Service Unit/Service Area

Copies of all forms must be retained by each Service Unit/Service Area together with all supporting documentation (and should be clearly marked "file copy"). In addition, the following shall be maintained within the Service Unit/Service Area in a secure place:

- the period over which surveillance occurred
- the frequency of reviews prescribed
- the results of each review
- the date & time of instructions given by the authorising officer

Such records shall be maintained for at least three years from the conclusion of the investigation or operation. It shall be the responsibility of Member of the Corporate Leadership Team with Management Responsibility for the relevant service unit/service area to ensure that such facilities are available for use and used in accordance with this procedure.

K. RETENTION OF PRODUCT

1. Confidential Information

Confidential personal information (information where a high degree of privacy may be expected due to the relationship between the parties concerned e.g. solicitor/client; priest/parishioner; journalist/informant; counsellor/consultee, etc) will not be acquired as a result of any covert surveillance, the use of CHIS and the acquisition and disclosure of communications employed by the council. Where there is any identified risk of acquiring confidential information prior to authorisation, then such activity shall not be authorised.

Any confidential information which is inadvertently obtained shall be destroyed forthwith.

2. Collateral Information

Collateral information (information about persons not connected with the investigation or prosecution) shall, wherever possible, be destroyed forthwith.

3. No Action Cases

Where information is acquired which does not ultimately give rise to a prosecution or any other action, it shall be destroyed, unless there is any likelihood of further action in the same matter at a later date.

4. Prosecution Cases

In all cases where a prosecution or other action is to be taken, the product acquired will be retained in order to comply with inter alia the Criminal Procedures and Investigations Act 1996.

5. Destruction of Product

Wherever any product is to be destroyed in accordance with this policy, it shall be done so in a secure and confidential manner, so as to avoid any information being divulged other than in accordance with the law.

L. CONCLUSION

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this document, will ensure that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. All applicants will be suitably trained and must when preparing an application for submission to an Authorising Officer have due regard to these issues.

4. Authorising officers will be suitably trained and they must exercise their minds every time they are asked to sign a form. They must never sign forms without thinking about their personal and the council's responsibilities. Careful consideration must be given to the potential for collateral intrusion.

5. Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

6. For further advice and assistance on RIPA, please contact the council's Corporate Director of Governance.

Appendix 1

List of authorised signatories

SENIOR AUTHORISING OFFICER
DESIGNATION
Chief Executive – Dave Heywood
AUTHORISING OFFICERS
DESIGNATION
Corporate Director – Chief Operating Officer – Jackie Smith
Corporate Director of Place and Communities – Annette Roberts

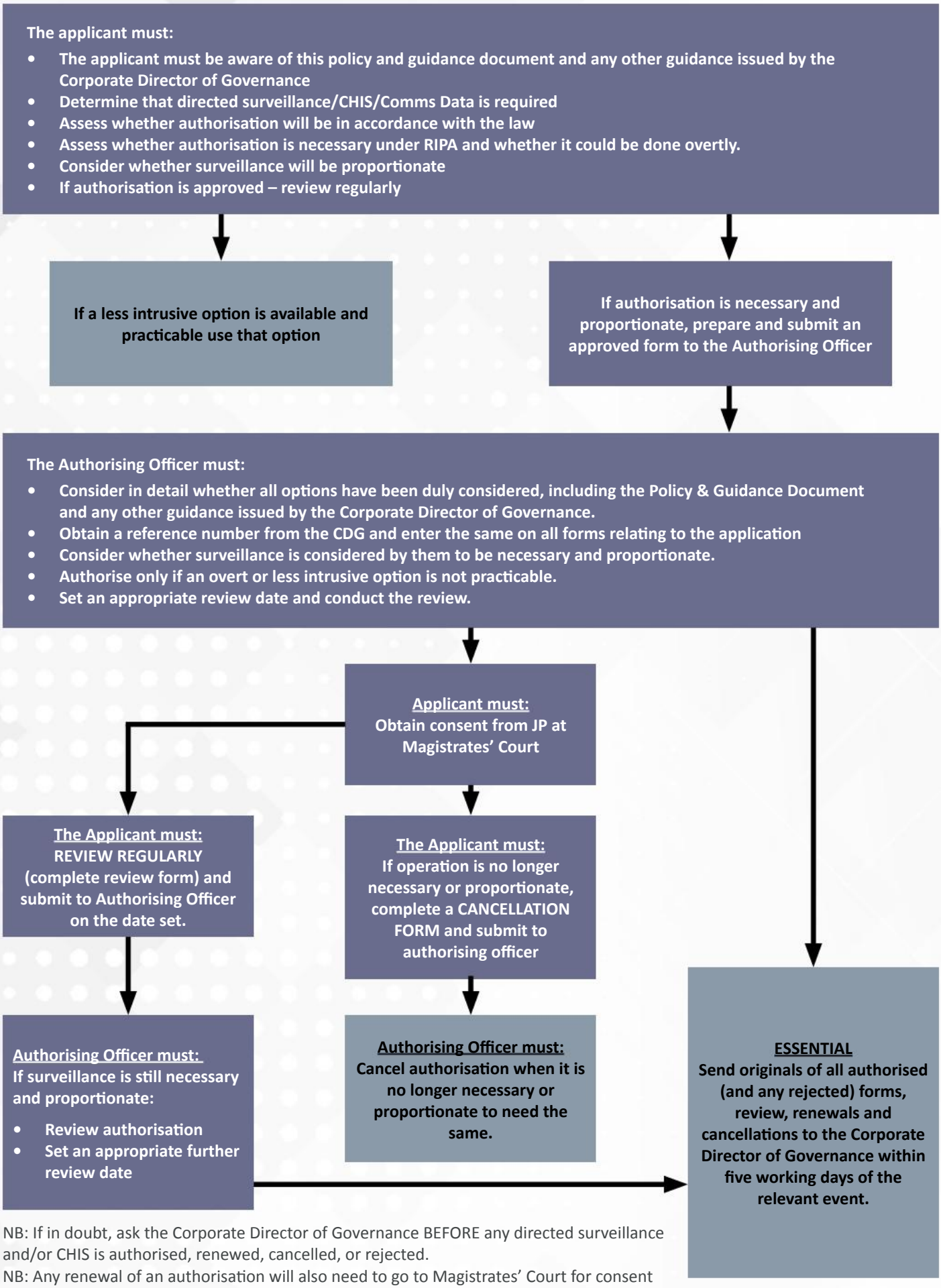
Notes:

1. Only the Chief Executive may sign authorisation relating to Juvenile Sources and vulnerable individuals and where a potential for the acquisition of confidential information has been identified.

2. Employee surveillance using covert surveillance may only be authorised by the Chief Executive.

3. An authorising officer may not sign an authorisation or give authorisation under the agency procedures relating to a service/activity for which he/she has management responsibility.

Appendix 2 - RIPA Flow Chart



NB: If in doubt, ask the Corporate Director of Governance BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.
NB: Any renewal of an authorisation will also need to go to Magistrates' Court for consent from a JP as for the original application.