EXECUTIVE
Monday, 2 September 2024
10.00 am
John Meikle Room, The Deane House, Belvedere Road, Taunton TA1 1HE

SUPPLEMENT TO THE AGENDA

To: The members of the Executive

We are now able to enclose the following information which was unavailable when the agenda was published:

This page is intentionally left blank

Somerset Council

IG 10~~9~~
Covert Surveillance (RIPA) Policy

Organisation	Somerset Council
Title	IG 109 Covert Surveillance (RIPA) Policy
Author	~~Rebecca Martin~~ Lesley Dolan
Owner	~~Rebecca Martin~~Lesley Dolan
Protective Marking	Official - Unclassified
Primary Legislation	GDPR Data Protection Act 2018 Regulation of Investigatory Powers Act 2016

Document Distribution

This document will be distributed to: **All Elected Members, Somerset County Council Staff, 3rd Party Contractors, Secondees and Volunteers**

Responsible	~~Officer~~Information Governance Manager
Accountable	~~SIRO~~SRO
Consulted	Corporate and Resources Scrutiny Committee~~Information Governance Board~~ Executive , ~~HR, Unions~~
Informed	All members, employees, contractors, volunteers and 3rd parties

Version History

Revision Date	Author	Version	Description of Revision
10/06/2021	Rebecca Martin	5.0	Recommendations from IPCO inspection
27/01/2023	Rebecca Martin	5.1	Roll over and rebrand for unitary
	Lesley Dolan	5.2	Recommendations from IPCO inspection 2024

Document Notification

Approval	Name	Date
Information Governance Manager	Rebecca Martin	27/01/2023
Chief Executive	Pat Flaherty	10/06/2021
SIRO	Simon Clifford	10/06/2021
HR	Chris Squire	10/06/2021
Unions	Via Vicky Hayter	10/06/2021

Document Contents Page

POLICY ON A PAGE

Somerset Council will ensure all users of Council systems and data have access to the rules that apply to conducting covert surveillance.

This document will be distributed to: **All employees and will be available on the intranet (SharePoint).**

Key Messages

- The Council shall ensure that covert surveillance is only undertaken where it complies fully with all applicable laws, the: Human Rights Act 1998, Investigatory Powers Act 2016, Data Protection Act 2018 and UK GDPR.
- The Council shall, in addition, have due regard to all official guidance and codes of practice particularly those issued by the Home Office, the Investigatory Powers Commissioners Office (IPCO), the Security Camera Commissioner and the Information Commissioner.
- Covert surveillance shall only be undertaken where it is absolutely necessary to achieve the desired aims; and shall only be undertaken where it is proportionate to do so and in a manner that it is proportionate.
- Be aware that systematic, repeated or regular visits to and viewing of citizens or employees Social Media sites, for the purpose of obtaining personal data, can be determined as covert surveillance.
- Adequate regard shall be had to the rights and freedoms of those who are not the target of the covert surveillance.
- All authorisations to carry out covert surveillance shall be granted by appropriately trained and designated authorising officers.
- RIPA authorisation of eligible covert surveillance is also subject to judicial approval.
- Adherence to this policy will minimise intrusion into citizens' lives and will avoid any legal challenge to possible covert surveillance activities undertaken by the Council

This "policy on a page" is a summary of the detailed policy document please ensure you read, understand and comply with the full policy.

1. Purpose

- To ensure that Somerset Council complies with the legal requirements of the applicable Acts and to have a uniform system to cover all relevant activities undertaken by Somerset Council.
- To ensure that surveillance and communications data is only sought for legitimate reasons and is necessary and proportionate to meet its aims.
- To ensure that only suitable and competent persons authorise covert surveillance.
- To ensure all Somerset Council employees are aware of the rules and procedures applicable to investigations involving covert surveillance.

2. Scope

This policy and procedure provide a framework to cover the authorisation of the following methods of covert surveillance:

- directed surveillance.
- acquisition and disclosure of communications data

It should be noted that the Council does not normally expect to be engaged in such covert surveillance activities for the following reasons:

- It is our policy is to inform Council employees of any investigation they may be subject to concerning fraud or computer misuse.
- Since May 2013 responsibility for conducting investigations concerning Trading Standards in Somerset has passed to Devon County Council
- It is our policy to ensure that all use of CCTV cameras by the Council is overt and not covert.

This policy replaces the Council's RIPA Surveillance and Monitoring Policy May 2013 and should be read in conjunction with the current Employee Monitoring and Surveillance Policy and council policies on use of the Internet and social media.

3. Policy

Procedure for authorising Covert Directed Surveillance and use of a Covert Human Intelligence Source (CHIS)

Covert Surveillance - means surveillance carried out in a manner designed to ensure that the person subject to the investigation is unaware it is taking place.

Directed Surveillance, - is covert surveillance, which is not intrusive[1] and is undertaken:

[1] **Intrusive Surveillance -** relates to surveillance taking place on any 'residential premises' (including a hotel bedroom) or in any private vehicle, the Council is not authorised to undertake intrusive surveillance.

- for the purposes of a **specific** investigation or operation and
- in such a manner that is **likely to obtain private information** about a person
- in a **planned** manner which enables prior authorisation to be reasonably sought.

A Covert Human Intelligence Source (CHIS) is an informant – a person who establishes or maintains a relationship with an individual for the purpose of gathering intelligence covertly. A CHIS under the age of 18 is referred to as a Juvenile CHIS.

All investigations involving covert directed surveillance activities or use of a CHIS must be authorised using the processes and forms attached to this policy.

Covert surveillance which concerns the prevention or detection of a serious criminal offence may be eligible for a **RIPA authorisation**. Rules and criteria for this are provided in Appendix 3.

Further advice on the authorisation process and principles (including sample application forms with guidance) is available from Information Governance.

Online covert activity

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever the internet is used as part of an investigation, consideration must be given as to whether the proposed activity is likely to interfere with a person's rights under the Human Rights Act, including the effect of any collateral intrusion. Any activity likely to interfere with such rights should only be used when necessary and proportionate to meet the objectives of a specific case. Wherever it is considered that private information is likely to be obtained, an authorisation must be sought (as set out elsewhere in this policy).

Social Networks

Social networking sites contain personal information about individuals. While the individual has effectively made this information "publicly available", it is, arguably, still "private information". Targeted collection of such information interferes with the person's right to a private life "in a public place", just as would the targeted filming of his/her movements on a public street.

Repeat viewing of particular sites for the purpose of intelligence gathering and data collection about an individual should therefore be considered as a form of covert surveillance, subject to the appropriate authorisation procedures (as set out in this policy).

With the departure of trading standards responsibilities, it is unlikely that the Council will use social media for investigatory purposes. Nevertheless, social media is

recognised as providing a source of helpful and sometimes invaluable intelligence and evidence for investigators. The likelihood is that those engaged in enforcement on behalf of the Council will find themselves attracted in the future to these sources and, if they do so, it is important that they are aware of those activities which attract authorisation.

Investigating officers should appreciate that researching “open source” sites will not attract authorisation unless they return to those sites on other occasions usually for the purpose of building a profile. In such cases, directed surveillance authorisation would be required.

If the officer breaches the privacy controls on the site by using a covert account not identifying himself as a Council officer, and becomes, e.g. a “friend” on Facebook, this will require at least directed surveillance authorisation.

If the officer thereafter makes direct contact with the owner/operator the site and thereby establishes a relationship, a CHIS authorisation would have to be obtained. Although the CHIS may do no more than engage through the Internet, a controller and handler together with a record keeper (who may be either controller or handler) must be appointed and a risk assessment drafted. (RIPA section 29(2)(c) and (5)). It follows that officers should be trained to act in these capacities although such training would not require them to reach the standard of commensurate police officers.
~~Attention is drawn to the 2014 edition of the OSC Procedures and Guidance Document, paragraph 288 for assistance in this field and in determining when RIPA authorisation is required.~~

Information Governance should be contacted for advice in this area.

Authorising Officers

The Authorising Officers (AOs) will normally arrange for the preparation of the additional papers and, as appropriate, attend, or arrange for an appropriate person to attend~~,~~ the Court to obtain Magistrates approval of the RIPA application. However, these hearings have the status of legal proceedings and the officer making the application to a Magistrate should be authorised under section 223 of the Local Government Act. The current Authorising Officers and the limits of their authority are contained in the attached schedule Appendix 1.

The persons named in the attached schedule Appendix 1. are responsible for granting or declining authorisations. They must **not** take part in any surveillance related to an application which they have authorised and must be sufficiently removed from the investigation that they can be deemed to manage it but are not involved with the day-to-day conduct.

The SRO is the only person in normal circumstances with authority to authorise directed surveillance where “confidential” information may be obtained.

Use of a Covert Human Intelligence Source (CHIS)

Although the regime of RIPA authorisations includes the use of a Covert Human Intelligence Source (CHIS) the Authority recognises the very onerous responsibilities placed on the CHIS handler and the lifelong duty of care owed to the CHIS. **It is therefore the *policy of this Authority only to consider the use of CHIS for surveillance purposes in exceptional circumstances*.**

Officers should be aware that gathering intelligence via a social networking site in situations where an officer uses a covert account to contact the subject of investigation or the officer uses such account to establish a relationship with the subject of investigation constitutes use of a CHIS, would be subject to authorisation and would only be considered by the authority in exceptional circumstances in line with the statement above. A controller and handler together with a record keeper (who may be either controller or handler) would also need to be appointed to manage such a CHIS. A risk assessment would also need to be drafted. (RIPA section 29(2)(c) and (5). Officers would need be trained to act in these capacities.

The authorisation of juvenile or vulnerable CHIS or the acquisition of confidential information may only be undertaken by the Head of Paid Service or whoever deputises for him in his absence.

Records, Central Authorisation Register and Quality Assurance
Officers named in the attached schedule (Appendix 1) shall keep records of all applications, authorisations, reviews and revocations etc. during the investigation. Copies of all authorisation documents will be passed to the RIPA Co-Ordinator , including authorisations which have been declined. On completion of the investigation and any appropriate follow up the documents will be destroyed, in accordance with Data Protection legislation.

The RIPA Co-ordinator will keep and review a register - the Central RIPA Authorisation Register. The Current RIPA Co-ordinator is identified in Appendix 1.

The Register will record and hold copies of all RIPA authorisations, reviews, renewals, cancellations and rejections for a period of at least 5 years. It must, on request, be made available for inspection by the Investigatory Powers Commissioners Office.

Communications Data (External & Internal)

Access to communications data is governed by 'The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000'.

Applications for access to communications data (phone and Internet subscriber details and itemised billing) are handled by the National Anti-Fraud Network's (NAFN) Single Point of Contact (SPoC) services. This is coordinated by Devon County Council under a collaboration arrangement which created a shared service with Somerset Council for this purpose.

The Council has an agreed policy governing the use of internet and email. This states that users, authorised or unauthorised, have no right of privacy regarding such use. Any request to monitor an individual's internet or telephone (laptop, desktop or a work mobile, handheld device e.g. smart phone) history/log and emails should be made to directly to ICT or via HR if the request is pertaining to an employee.

Further Information and Guidance

Further guidance on surveillance can be found in the following ***Home Office Codes of Practice:***

Code of Practice for Covert Surveillance and Property Interference

Code of Practice for Covert Human Intelligence Sources

Code of Practice for the Interception of Communications

Code of Practice for Investigation of Protected Electronic Information

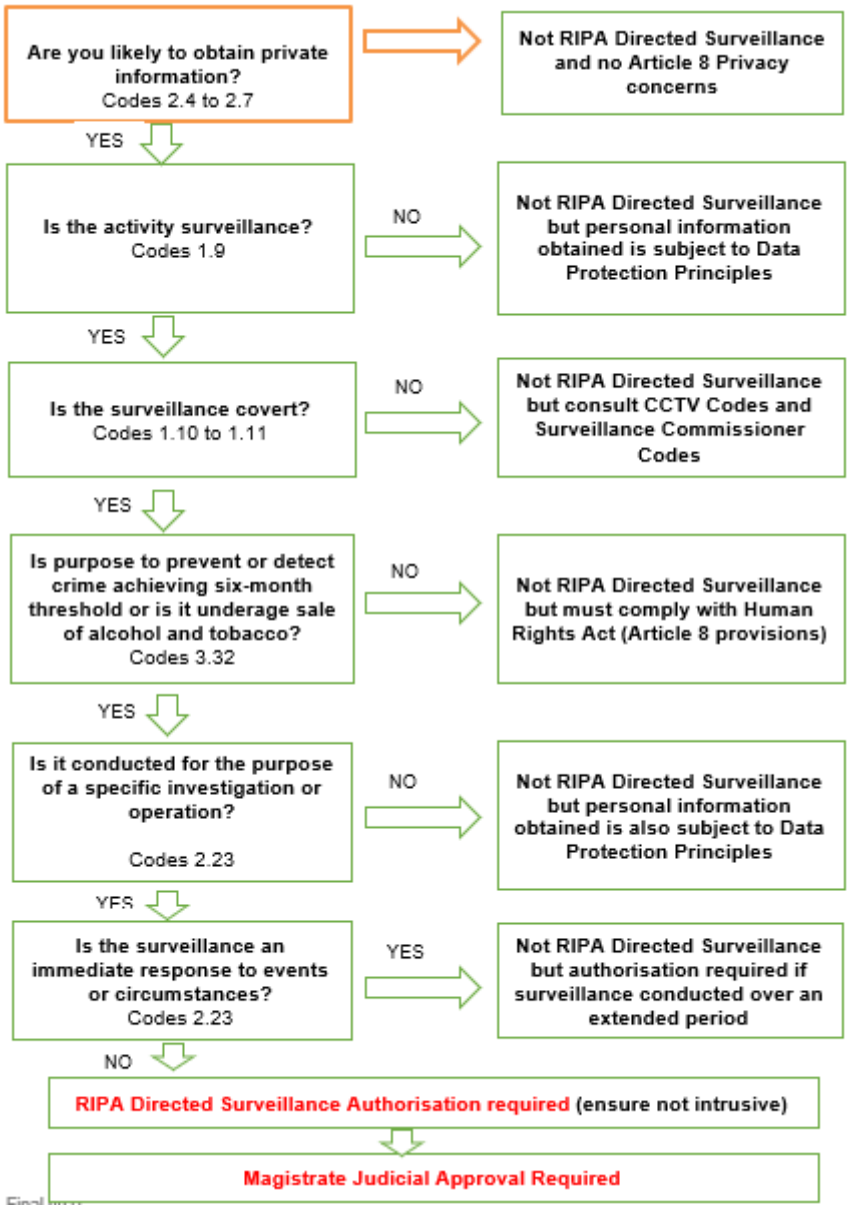
Codes of Practice for the acquisition, disclosure and retention of communications data

Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012

Section 6 of the SWERCOTS Enforcement and Legal Process Manual also contains comprehensive advice on the law and best practice relating to RIPA and should be consulted in addition to this policy and the guidance in the following appendices.

Directed Surveillance Decision Chart

The flow chart on the following page illustrates the decision-making process which should be followed when considering investigations involving directed surveillance:


Are you likely to obtain private information?
Codes 2.4 to 2.7
Not RIPA Directed Surveillance and no Article 8 Privacy concerns
YES
Is the activity surveillance?
Codes 1.9
NO
Not RIPA Directed Surveillance but personal information obtained is subject to Data Protection Principles
YES
Is the surveillance covert?
Codes 1.10 to 1.11
NO
Not RIPA Directed Surveillance but consult CCTV Codes and Surveillance Commissioner Codes
YES
Is purpose to prevent or detect crime achieving six-month threshold or is it underage sale of alcohol and tobacco?
Codes 3.32
NO
Not RIPA Directed Surveillance but must comply with Human Rights Act (Article 8 provisions)
YES
Is it conducted for the purpose of a specific investigation or operation?
Codes 2.23
NO
Not RIPA Directed Surveillance but personal information obtained is also subject to Data Protection Principles
YES
Is the surveillance an immediate response to events or circumstances?
Codes 2.23
YES
Not RIPA Directed Surveillance but authorisation required if surveillance conducted over an extended period
NO
RIPA Directed Surveillance Authorisation required (ensure not intrusive)
Magistrate Judicial Approval Required

4. Governance Arrangements

7.1 Policy Compliance
If any employee is found to have breached this policy, they may be subject to Somerset Council's disciplinary procedure.

Where it is considered that a criminal offence has potentially been committed, the Council will consider the need to refer the matter to the police.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Governance Team

7.2 Policy Governance
The following table identifies who within Somerset Council is accountable, responsible, informed or consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation.
- **Informed** – the person(s) or groups to be informed after policy implementation.

Responsible	Information Governance Manager
Accountable	SIRO
Consulted	Information Governance Board, HR, Unions
Informed	All members, employees, contractors, volunteers and 3rd parties

7.3 Review and Revision
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by the Information Governance Manager or Data Protection Officer.

In line with paragraph 4.47 of the Covert Surveillance and Property Interference Code of Practice the revised policy will be reviewed and adopted by Elected Members ~~-~~annually, through Executive ~~Cabinet~~ Member decision following presentation and discussion at Corporate and Resources Scrutiny ~~Place~~ Committee.

Appendix 1 – Nominated Officers

RIPA Co-ordinator
01/04/2021

Name	Title	Designation
~~Rebecca Martin~~	Information Governance Manager	RIPA co-ordinator

Schedule of Authorising Officers for Covert Surveillance
01/04/2021

Name	Title	Designation
Duncan Sharkey	CEO and Head of the Paid Service	Authorising Officer for CHIS applications
~~Chris Squire~~ David Clerk	~~Director (HR) & Senior Information Risk Owner (SIRO)~~ Service Director, Governance, Legal and Democratic Services	~~Senior Responsible Officer~~ Senior Responsible Officer
~~Vicky Hayter~~ TBC	~~Strategic Manager for HR~~	Authorising Officer
~~Dave Littlewood~~TBC	~~Strategic Manager – ICT~~TBC	Authorising Officer
National Anti-Fraud Network (NAFN) **	Devon County Council, Trading Standards	SPoC (Single Point of Contact)

** Somerset Council is a member of NAFN and will use the service as the Single Point of Contact (SPoC) in respect of communications data.

Appendix 2 – Authorising Directed Surveillance: Rules and Criteria

AUTHORISING DIRECTED SURVEILLANCE: RULES AND CRITERIA

Section 27 of RIPA provides a powerful defence if covert surveillance is challenged:

> *"(1) Conduct to which this Part applies shall be lawful for all purposes if -*
> *(a) an authorisation under this Part confers an entitlement to engage in that conduct on the person whose conduct it is; and*
> *(b) his conduct is in accordance with the authorisation."*

To take advantage of this defence, the surveillance needs to be properly authorised. S.28 sets out the criteria for authorising Directed Surveillance, whilst S.29 covers CHIS.

The Authorising Officer
The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 N0.521) states that the Authorising Officer for a local authority can be a Director, Head of Service, Service Manager or equivalent.

Where the surveillance involves the likelihood of obtaining confidential information or the deployment of juveniles or vulnerable people, then the authorisation has to be sought from the Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

If there is any doubt regarding sufficiency of rank you should contact your Legal Section or RIPA Co-ordinator for advice.

Time Limits
The current time limits for an authorisation are 3 months for Directed Surveillance and 12 months for a CHIS (4 months if the CHIS is underage).

The duration of any authorisation commences with the magistrate's approval.
A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by a Magistrate.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but local authorities must take account of factors, which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a Magistrate to consider the application).

Authorising Officer's Consideration

(Chapter 3, Covert Surveillance Code) S.28(2) states:

> *"A person shall not grant an authorisation for the carrying out of directed surveillance unless he believes -*
> *(a) that the authorisation is necessary on grounds falling within subsection (3); and*
> *(b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out."*

Please consult flowchart 4 when deciding whether Directed Surveillance should be authorised.

The first question that the Authorising Officer needs to ask is; Is the surveillance necessary?

The surveillance has to be necessary on one of the grounds set out within S.28(3). Previously local authorities could authorise Directed Surveillance where it was necessary "

> "for the purpose of preventing or detecting crime or of preventing disorder." (S.28(3)(b))

The Home Office Review, which reported in January 2011, recommended that where local authorities wish to use Directed Surveillance, this should be confined to cases where the offence under investigation is a serious offence.

This recommendation was put into effect by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 which was made in June 2012 and came into force on 1st November 2012. This amends the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521 ("the 2010 Order"), which prescribes which officers, within a public authority, have the power to grant authorisations for the carrying out of Directed Surveillance and the grounds, under Section 28(3), upon which authorisations can be granted.

From 1st November 2012, local authority Authorising Officers may not authorise Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and it meets the condition set out in New Article 7A(3)(a) or (b) of the 2010 Order. Those conditions are that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of **at least 6 months of imprisonment**, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. The latter are all offences involving sale of tobacco and alcohol to underage children.
So what about surveillance being carried out to tackle disorder (e.g. anti social behaviour)? This can no longer be authorised as Directed Surveillance unless the disorder includes criminal offences satisfying the above criteria.

The second question is; Is the surveillance proportionate to what is sought to be achieved by carrying it out?

Proportionality means ensuring that the surveillance is the least intrusive method to obtain the required information having considered all reasonable alternatives. This requires consideration of not only whether surveillance is appropriate but also the method to be adopted, the duration and the equipment to be used.

The OSC often states in its inspection reports that officers have not properly understood this concept or have not demonstrated compliance within the authorisation form. The Covert Surveillance Code (para 3.6) requires four aspects to be addressed in the authorisation form:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented. The third question is; Can we avoid or minimise collateral intrusion?

The third question is; Can we avoid or minimise collateral intrusion?

The Authorising Officer will need to carefully consider the likelihood of collateral intrusion occurring. This is the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation. If the risk is significant, measures should be taken, wherever practicable, to avoid or minimise any unnecessary intrusion.

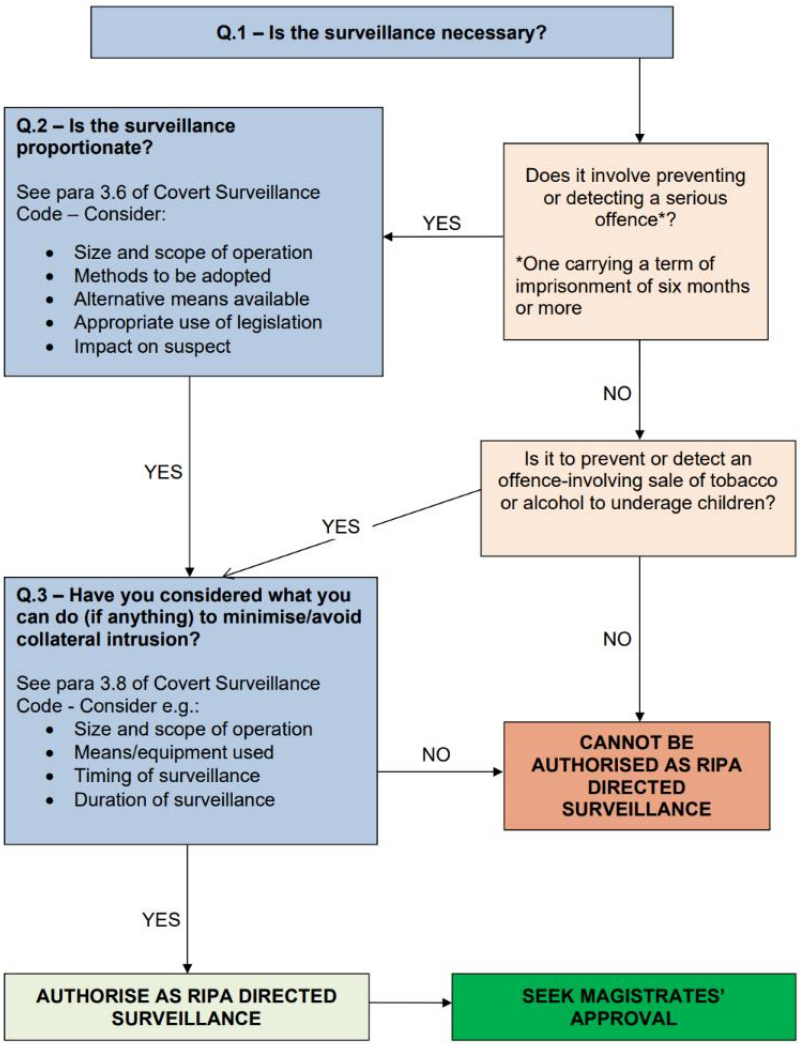
Investigating and Authorising Officers will need to ask themselves:

- What is the impact on third parties? Is it significant?
- If it is, what can be done to avoid or minimise it?
- Have we considered:
    - Changing the timing of the surveillance
    - Reducing the amount of surveillance
    - Changing the method of surveillance
    - The sensitivities of the local community
    - Surveillance operations by other public authorities

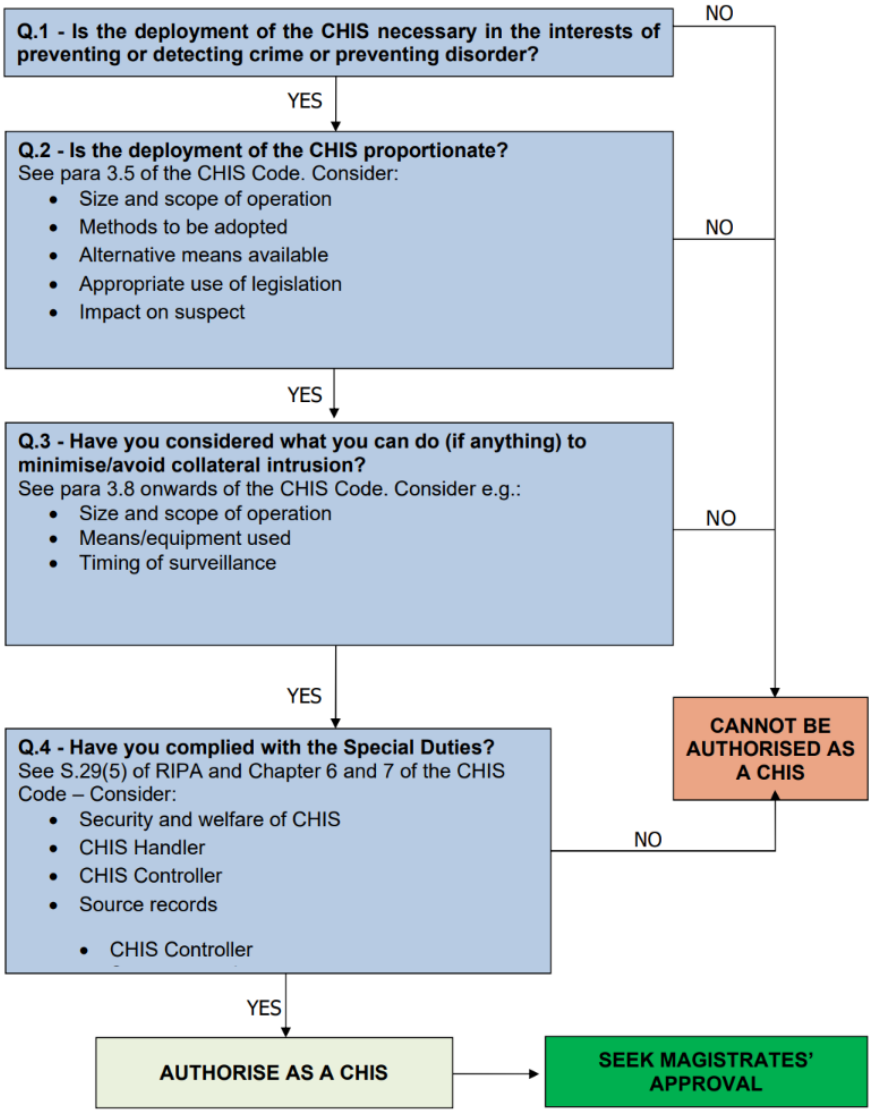
Of course at all times the need to obtain the best evidence to investigate the crime will be paramount.

Next Stage: Once the surveillance has been authorised the next stage is to seek Magistrates' approval. See section 8 for a detailed explanation of the procedure

Flowchart 4 – Authorising Directed Surveillance (RIPA)



Flowchart 5 – Authorising a CHIS



Appendix 3 – Non-RIPA Surveillance

NON-RIPA SURVEILLANCE

The Council does not anticipate conducting covert surveillance which is not eligible for a RIPA authorisation.

- The authorisation under RIPA affords a public authority a legal defence under Section 27. This means the activity will be lawful for all purposes.
- While use of covert surveillance without the protection of a RIPA authorisation will not necessarily be illegal, such use of covert surveillance risks breaching legislation on Human Rights and/or Data Protection (see below).

Covert surveillance activity in the following areas should not be undertaken without the advice of the SRO, the RIPA Co-ordinating Officer and the Legal Services:

1. Crimes Not Carrying Six Months Imprisonment

From 1st November 2012, local authority Authorising Officers may not authorise Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and it meets the condition set out in New Article 7A(3)(a) or (b) of the 2010 Order. Those conditions are that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (offences involving sale of tobacco and alcohol to underage children).

The higher threshold in this legislation reduces the number of cases in which local authorities have the protection of RIPA when conducting covert surveillance.

2. Employee Surveillance

Following a decision by the Investigatory Powers Tribunal, it should be understood that employee surveillance will generally not be capable of authorisation ~~ble~~ under RIPA.

In C v The Police and the Secretary of State for the Home Department (14th November 2006, No: IPT/03/32/H), the Tribunal ruled that this was not the type of surveillance that RIPA was meant to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

"The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the

Formatted: Underline

regulation of employees or of suppliers and service providers."

Appendix 4 – Somerset Council Guidance Handbook

SOMERSET COUNCIL GUIDANCE HANDBOOK

Regulation of Investigatory Powers Act 2016 (RIPA)

Contents

1. The RIPA Authorisation Procedure

Responsibilities of Applicants and Authorising Officers when Assessing and completing the Application Form.

The Authorising Officer must;

- Consider each application on its own merit using the Covert Surveillance Code of Practice and the Acquisition and Disclosure of Communications Data Code of Practice.
- Ensure the application form is comprehensively completed
- Demonstrate clearly and succinctly how the investigation is necessary on the criminal threshold grounds, proportionate and is the most appropriate method to achieve the objective.
- Ensure the forms detail any collateral information that may be obtained, how that will be minimised, and what will happen to that information to protect the information of other private individuals.
- As appropriate arrange for approval by a Magistrate or,
- Issue a rejection.
- Ensure that the necessary procedures to obtain judicial authorisation are followed.
- Conduct frequent reviews of the investigation and issue cancellation or renewal notices as appropriate. A cancellation notice must be issued when the authorisation has expired, or the investigation is completed.
- Forward copies of all documentation to the RIPA Co-ordinator.

The Applicant must;

- Complete the application correctly and obtain approval from their Service Manager before submitting the application to an Authorising Officer, and additionally, in the case of communication data, to NAFN as the SPoC to check legal compliance. (NAFN will then forward application to the Authorising Officer/Designated Person to organise approval by a Magistrate).
- Use and obtain the data only for the purpose and by the method stated.
- Only obtain the minimum data that is necessary and proportionate for the purpose stated.
- Ensure that data collected is kept secure, not passed to anyone else for purposes other than that stated, and is destroyed appropriately.

Completion of the RIPA Authorisation Forms.

All applicants are responsible for completing correctly the relevant forms and submitting them via their Service Manager to the relevant person for authorisation. (Communications Data via NAFN, Authorising Officer). For employee focused investigations please seek advice from the appropriate HR Adviser as soon as possible.

The Authorising Officer must ensure they are eligible to consider an application, see the schedule of Authorising Officers in the RIPA Policy, and the Service Manager has approved the investigation.

Consideration of the Application

The authorising officer shall consider each application on its own merit using the guidance they have received in corporate policies and procedures, training and the Covert Surveillance Code of Practice, the Covert Human Intelligence Sources Code of Practice and the Acquisition and Disclosure of Communications Data Code of Practice.

The Authorising Officer must then check that the appropriate application form has been comprehensively completed. The application should demonstrate the investigation is required to detect /prevent a crime and meets the four test elements of directed surveillance;

- covert (the subject is unaware),
- planned
- specific
- likely to obtain private information.

The applications should show clearly and succinctly how the investigation is necessary, proportionate and the most appropriate method to achieve its objective. Ideally it should state the relevant legislation to demonstrate the criminal activity the investigation is seeking to detect or prevent, and, where appropriate, include other options considered but discounted as not being able to deliver the objective.

The authorising officer must consider the activity to be;

- necessary on the lawful ground of 'the purpose of preventing or detecting crime, or preventing disorder; and
- proportionate to what is trying to achieve; and
- the most appropriate method to achieve the objective (subsidiary).
- Consideration should be given to other methods, which could be used to achieve the objective.

The application should also detail any collateral information that may be obtained, how that will be minimised, and what will happen to that information to protect the information of other private individuals.

Granting or Declining an Authorisation

If the Authorising Officer (AO) supports the application, they shall complete the application form appropriately, advise the applicant that judicial approval is to be sought and then obtain that approval. The onus is on the Authorising Officer to satisfy themselves (and record the factors they have considered) that the investigation requires directed surveillance and meets the tests of necessary, proportionality and subsidiary.

The AO is required to demonstrate they have considered the balance between the intrusiveness of the activity, both on the target and others who might be affected, against the need for the activity in operational terms. Also that the activity is not considered to be excessive i.e. a sledgehammer is not being used to crack a nut! An audit trail must be kept of the decision making process and include details of any amendments made as the process progresses, e.g. changes to the period of surveillance. The RIPA Co-ordinator must be provided with all the documents.

Should the application fail any of the above three tests (necessary, proportionate and subsidiary), or is not considered to be directed surveillance RIPA Authorisation may not be granted and a record should be made of the decision, including reasoning, to reject. The RIPA Co-ordinator must be provided with all the documents.

Following authorisation by the Authorising Officer the application must be sent for judicial authorisation before any surveillance activity can begin.

The Authorising Officer will arrange for the application to go before a magistrate to obtain authorisation, represented by a designated Local Authority Officer (Section 223 Local Government Act 1972), before an investigation starts, ensuring Local Authority compliance with the Home Office Guidance and Magistrates Court compliance in respect of these applications.
The Authorising Officer must be sufficiently removed from the investigation to have an objective view of the proposed surveillance.

IPCO does not recommended that the SRO is designated as an Authorising Officer.

The Authorising Officer will forward the judicially approved application to the

applicant and the RIPA Co-Ordinator. The Authorisation Officer should confirm the dates to review the authorisation with the applicant.

Post Authorisation

The Authorising Officer is also required to review all investigations at timely intervals appropriate to the surveillance activity undertaken or within a maximum period of 28 days. Frequent review is recommended and renewal authorisation or cancellations should be issued (using the appropriate documents) to demonstrate the consideration given at the review. A Judicial Review is required for any renewals.

After authorisation, the applicant is responsible for obtaining and using the data only by the method and for the purpose stated in the authorisation. They should obtain only the minimum amount of data necessary and proportionate for the purpose stated. They are also responsible for ensuring that the data is kept secure, is not passed to anyone else for purposes other than those for which it was obtained is destroyed appropriately.

When the authorisation is cancelled (this may or may not be at the conclusion of the surveillance or investigation) the Authorising Officer shall retain the RIPA documentation for safekeeping and issue a cancellation notice. Copies of all documentation, including cancellations, should also be filed on the Central RIPA Authorisation Register held by the RIPA Co-ordinator. A unique reference number will be allocated by the RIPA Co-ordinator for each application against which the application will be recorded.

The authorisation will remain valid for a maximum of three months from the date of issue (directed surveillance) and 1 month (CHIS). If the surveillance and monitoring activity is not completed within that period, the applicant shall, as soon as possible, apply to the Authorising Officer to renew the authorisation. See 4.1 above and note that Judicial Approval will run from the expiry of the original authorisation. Applicants should therefore consider factors which might delay a renewal e.g. availability of a magistrate during a week end or public holiday.

RIPA Applications and Forms

Available here:
https://www.gov.uk/government/collections/ripa-forms--2

2. Appointing Authorising Officers and their Responsibilities

The Senior Responsible Officer's Responsibilities

The Senior Responsible Officer (SRO) will be a Director level officer.

The SRO is responsible for ensuring Somerset Council complies with the terms of RIPA and establishing best practice within the Council.

This responsibility includes:

- Policy development and implementation
- Administration and maintenance of a central record of authorisation (via the RIPA Co-ordinator)
- Training and Updates as appropriate
- Quality control (RIPA Co-ordinator).
- Liaison Officer for the Investigatory Powers Commissioners Office (IPCO) including reports as requested.

The SRO shall also have specific responsibility for

- Appointment of authorising officers (AOs) and the RIPA Co-ordinator;
- ensuring the quality and training of authorising officers (AOs) and
- general oversight of the authorisation process.

In the appointment of AOs the SRO will consider candidates proposed by the Executive Leadership Team (ELT). Deliberations in this regard will include the individual's job role, capacity, including their corporate responsibilities and their experience of sensitive investigations.

The RIPA Co-ordinator Responsibilities

Responsibilities of the RIPA Co-ordinator include:

- maintaining the Central Record of Authorisations and 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.
- monthly review of any current authorisations

The RIPA Co-ordinator receives, within one week of issue, copies of all authorisations, rejections, renewals and cancellations to be held on a Central Register. On receipt of the application the RIPA Co-ordinator will issue a unique reference number in respect of that application to the AO.

The RIPA Co-ordinator will examine all forms on the Central Register for compliance with the law, legislation and any guidance, which may be issued from time to time in relation to RIPA. Should the RIPA Co-ordinator find any issue or problems with the authorisations the appropriate AO will be notified and the matter remedied.

Appointment of Authorising Officers /RIPA Co-ordinator

The SRO shall appoint authorising officers after receiving nominations from ELT.

The nominees' job role and responsibilities within Somerset Council are considered together with their experience in conducting sensitive investigations.

Candidates from an ICT and HR background are more likely to have the relevant experience, as these service areas have a concentration of personnel with expertise in conducting formal investigations. They are also the service areas that are more likely to require RIPA authorisation for investigations.

Other named authorising officers are then advised of the appointment and, where appropriate, changes are made to all relevant documentation to reflect the new appointment.

All authorising officers should receive appropriate training before taking up their Responsibilities.

Who are the Authorising Officers?

The Authorising Officers are listed in Appendix 2.

Responsibilities of Authorising Officers

The Authorising Officers are responsible for ensuring that the investigation is carried out in a manner which does not contravene the Act and minimises any intrusion on the subject's or other party's privacy. They must satisfy themselves by challenging the method proposed by the applicant that the investigation is necessary, and the information cannot be obtained in another way.

Replacement of Authorising Officers

If the Authorising Officers are no longer able to undertake their duties, they must advise the SRO, who will make the necessary arrangements to replace them with a suitably qualified individual.

Ensuring Best Practice

Reviewing the Procedures – The RIPA Co-ordinator holds a Central Register of Authorisations and periodically reviews the authorisations, renewals and cancellations issued by the Authorising Officers.

The SRO, AOs, Information Governance Manager and the RIPA Co-ordinator together with representatives from the Services, HR and ICT meet annually (in June) with the County Solicitor to review investigations which have been undertaken, the processes for seeking authorisation, and the relevant policies.

Training;

- Appropriate training materials will be supplied to all authorising officers for self-directed learning (supported by the Information Governance Manager). Training materials will be reviewed with the policy and following any changes in legislation or procedure.
- Authorising Officers will be available for direct advice.
- NAFN will provide the 'SPoC's for communications data for Somerset Coucil.
- Further information may be obtained from National Anti-Fraud Network (NAFN), Southwest of England Regional Co-ordination of Trading Standards (SWERCOTS) or other external sources.

3. FAQs for Managers seeking RIPA authorisations

These questions and answers outline;

- the background to the legislation
- the policies in place in response to legislative framework for investigations requiring surveillance and monitoring.
- the procedure to be followed when RIPA Authorisation is sought within Somerset Council.

What is R.I.P.A.?
R.I.P.A. is an acronym for the Regulation of Investigatory Powers Act 2016. The Act provides for a framework for Public Authorities to use certain surveillance and monitoring techniques which are compatible with the ECHR Directive.

When might the Council undertake surveillance and monitoring as part of an investigation?
Some aspects of a Local Authority work require surveillance to be undertaken. This is primarily to protect the public by preventing or detecting a crime. For example, authorisation may be required before a community protection officer could observe a suspected car dealer 'selling cars' from a private address or if an employee is suspected of criminally abusive behaviour towards a child or vulnerable adult or stealing from or defrauding the Council.

When might RIPA Authorisation be required?
When surveillance or monitoring is used as part of an investigation to prevent / detect a crime (including prevention of public disorder) and meets the criminal threshold and also the four test elements of:

- covert –the subject is unaware
- planned
- specific
- likely to obtain private information

For example, an investigation to determine if an employee or a member of the public had seriously defrauded the Council, which required the individual or their home to be watched, would necessitate an authorisation.

Do I need RIPA Authorisation if a third party is undertaking the investigation?

Yes. It is the responsibility of the Council to ensure that when surveillance is undertaken within the parameters of question 3 above that authorisation is sought. For example if the Council engaged a private detective to undertake an investigation into a matter where an employee or member of the public were suspected of defrauding the Council and the investigation met the criminal threshold plus the test elements of covert , planned, specific and likely to obtain private information, an authorisation would be required.

Who may authorise surveillance on an employee?
The RIPA authorisation process is used infrequently in the Council, and it is rarely required when an investigation into the behaviour of an employee is instigated.

However, to ensure due consideration of an investigation process, which may meet criteria requiring a RIPA Authorisation (see question 3) only the individuals trained and named in the Corporate Surveillance and Monitoring policy (Appendix1) may authorise directed surveillance. Such surveillance, where the subject is an employee, must be authorised by the Director, HR and OD or the named alternative specified within the Policy. Managers seeking such authorisation should seek advice from the HR Service prior to making an application.

For a list of current Authorising Officers please refer to the Covert Surveillance (RIPA) Policy, Appendix 2. If the information to be obtained is considered to be of a medical, spiritual, journalistic or legal privilege (Confidential Information) nature then normally only the Chief Executive may authorise an investigation.

Investigations relating to an employee should be authorised by the named authorising officers in HR.

All other investigations requiring authorisation must be authorised by a named authorising officer for criminal investigations.

For a list of current Authorising Officers please refer to the Corporate Surveillance and Monitoring Policy, Appendix 2

What is 'Confidential Information' and who may authorise investigations where this information may be obtained?
If the information to be obtained is considered to be of a medical, spiritual, journalistic or legal privilege (Confidential Information) nature then normally only the Chief Executive may authorise an investigation.

Is R.I.P.A. authorisation required to investigate Email, Internet or Telephone Abuse within Somerset Council
The Information Governance Policies, which all users are advised to read, state that 'all e-mails and activities on IT systems are subject to scrutiny by Somerset Council' therefore users cannot expect privacy. Employees are also periodically reminded of the main points in the Information Governance Policies and encouraged to read the full text. The Policy includes the Council's telephone systems. RIPA Authorisation would therefore be unnecessary as accessing an employee's email or

intranet log would not be 'covert'.

Monitoring of Somerset Council IT systems for business purposes i.e. examining the traffic of phone, internet or email use, is not covert and does not require R.I.P.A. authorisation. If it is necessary to open a person's Outlook Account (email box), it is preferable to advise the person before doing so. If in doubt RIPA Authorisation should be considered and advice sought.

As some schools do not have the IT Usage 'pop-up' when logging on to the IT system, RIPA should also be sought in investigations where the criminal threshold and the 4 test elements are met.

What would be considered to be abuse if IT Systems?
Guidance on how to avoid inappropriate use of ICT systems can be found in the Information Governance policies on the Somerset Council intranet site (SharePoint). If in doubt please seek guidance from your HR Service or from an Authorising Officer.

What should an Investigating Officer do to obtain authorisation?
The Investigating Officer (Applicant) must complete an 'Application for Authorisation' form. Care should be taken to use the correct form and forms may be downloaded from https://osc.independent.gov.uk/. Additional help may be found in this Handbook.

Forms are available for the following types of surveillance:

- Communications (external phone & internet access details)
- Directed surveillance (surveillance carried out covertly on a specific person, or for general surveillance for a specific reason)

The appropriate Service Manager should approve the investigation before the application for authorisation is made to a named Authorising Officer (see Covert Surveillance (RIPA) Policy, Appendix 2, Schedule of Authorising Officers) or, in respect of Communication Data, NAFN.

The application should be submitted to the appropriate Authorising Officer who, subject to approving the investigation, will arrange for the application to go before a magistrate to obtain authorisation before an investigation starts. The Authorising Officer must be sufficiently removed from the investigation to have an objective view of the proposed surveillance.

Does the Investigating Officer (applicant) have any responsibilities once authorisation has been granted?
After authorisation has been obtained, the Applicant is responsible for using the method in the authorisation to obtain only the minimum amount of information necessary to establish the evidence and ensure this is proportionate to what is trying to be achieved.

The data obtained must be used for the purpose stated on the application.

If, during the investigation, the original reason for requiring RIPA Authorisation changes e.g. to include a wider surveillance or from directed to CHIS surveillance, the original authorisation should be renewed or new authorisation sought as appropriate.

The applicant is also responsible for ensuring that the data is kept secure, is not passed to anyone else for other purposes than that stated and is destroyed appropriately.

The investigation should be reviewed regularly but, in any case, within three months, with the Authorising Officer and renewal or cancellation sought.

Applications requiring the use of a covert human intelligence source (CHIS) should be at least reviewed monthly but in normal circumstance weekly would be more appropriate.

During the investigation it is recommended that the investigating officer keeps a log of the material uncovered; the dates it was obtained and the date and method of destruction. Similarly, the way in which a CHIS is managed and protected should be documented together with the risk assessment process. At the end of the investigation the Authorising Officer must cancel the 'Authorisation'.

THE GOLDEN RULE:

If in doubt seek authorisation and advice

4. Guidance on Completing a RIPA Application

When seeking authorisation for directed surveillance it is essential that the forms be completed fully and clearly. The guidance below indicates the type of information required. Once the forms have been completed, they should be approved by the Service Manager and submitted to the Authorising Officer to check for legal compliance and arrange for approval by a Magistrate. In normal circumstances directed surveillance should not proceed before authorisation has been obtained, (Magistrate approval will depend on availability of a local Magistrate but in general can be obtained within 24 hours).

What is the specific purpose of the investigation?

- What are you asking to do and why? You are only able to do what you are authorised on the form to do.
- Provide details of the investigation and the enquiries to date.
- State the objectives of the investigation and the surveillance required to achieve the objectives.
- State how the criminal threshold is met.

Example - This investigation requires directed surveillance, which will involve both static and mobile surveillance & the use of video equipment on the subject.

- The investigation involves the potential serious offences of ----------and meets the criminal threshold as the potential maximum tariff is ----
- Legislation being considered ----------
- The objective of the investigation is to ----------
- Enquires carried out to date are---------- and they have established—

Details of the Surveillance

- State the static, foot mobile surveillance (visual) on (address of premises)
- State the intentions of surveillance (e.g. “observe and record the selling of stolen goods”)
- State when the surveillance is to take place
- State the equipment to be used (camera, video camera, CCTV)

Remember you can only carry out actions or use the equipment stated in the authorisation.

What information is expected to be gained from the surveillance?

- To gather intelligence and evidence to establish the extent of the criminality
- Identify other persons involved e.g. suppliers
- Identify premises involved e.g. for storage
- Identify the method the suspected criminal activity is carried out in
- Obtain evidence to assist with a prosecution of offenders
- Obtain best evidence as to the identity of persons responsible for the suspected crime.

The Grounds for seeking authorisation for Directed Surveillance
The only reason for which the Council may authorise directed surveillance is for the purpose of preventing or detecting crime or of preventing disorder.

Why is Directed Surveillance necessary?

- What other enquiries have been carried out & results?
- What other methods have been tried & failed?
- Why is this the only option?
- Overt enquiries will lead to the subject knowing of the investigation.
- Covert surveillance required to protect the source
- May reduce collateral intrusion by shortening the length of the investigation
- Serious nature of the offence
- If not authorised offences may continue without the required evidence to prosecute the offenders

Details of potential collateral intrusion, why it is unavoidable and how it may be minimised.
There may be collateral intrusions on neighbours, family, members of the public, other employees, customers;

Where collateral intrusion cannot be avoided it will be kept to a minimum by

- Only using sufficient trained staff to achieve the objectives.
- The surveillance will be focused on the specified subject/location with set objectives thereby reducing the collateral intrusion on members of the public.
- The focus of the operation will be solely on the subject, or any other person identified as being potentially involved.
- The surveillance will cease once the objectives have been achieved
- Photographic equipment will only be used at specified times as needed for evidence and intelligence gathering purposes. The equipment will focus on the subject and the activity taking place.

The same proportionality test applies to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

Officers 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 is required.

Why is this directed surveillance proportionate to what it seeks to achieve?

- Are you asking to do a lot to achieve a little? Are you using a sledgehammer to crack a nut?
- The serious nature (criminal offence punishable by ----------)
- Length of time of the surveillance operation
- Only method available with other options considered and discounted

- Consequences of not taking actions
- Surveillance will ultimately lead to prosecution and prevention

Will confidential material be obtained?
Is there a likelihood of medical, spiritual, legal or journalistic privileged information being obtained? If so a higher level of authority is required from the Chief Executive. The completed application will be processed by the Authorising Officer.

5. Useful Definitions

Surveillance - includes monitoring, observing or listening to persons, their movements, their conversations or their activities or communications, recording anything monitored, observed or listened to, or involving the use of a surveillance device. For the purposes of RIPA, the term 'persons' includes 'any organisation and any association or combination of persons'.

Surveillance, including covert surveillance, in itself does not require RIPA Authorisation but directed surveillance where criminal activity is suspected does.

Covert Surveillance - means surveillance carried out in a manner designed to ensure that the person subject to the investigation is unaware it is taking place. For Example: Most test purchases (where officers behave no different from a normal member of the public).

Directed Surveillance, - for the purposes of RIPA is covert surveillance, which is not intrusive and is undertaken:

- for the purposes of a specific investigation or operation and
- in such a manner that is likely to obtain private information about a person (whether or not one is specially identified for the purposes of the investigation or operation) and
- in a planned manner which enables prior authorisation to be reasonably sought.

For Example: A test purchase where the officer has a hidden camera to record information, which might include information about the private life of the shop owner.

Intrusive Surveillance - is covert and relates to surveillance taking place on any 'Residential premises' (including a hotel bedroom) or in any private vehicle; and

- involves the presence of an individual on the premises or in the vehicle or is carried out by means of surveillance a device ;or
- is carried out by means of a surveillance device in relation to anything taking place in any residential premises or in any vehicle but is carried out without a device being present on the premises or in the vehicle . The device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. An observation post outside the premises which provides a

limited view and no sound of what is happening inside would not be intrusive surveillance

The Council does not, under any circumstances, have the power to undertake 'Intrusive Surveillance'.

Communication data - relating to external postal service or telecommunications system (phones, faxes and internet usage). The only data that can legitimately be obtained for local authorities are:-

- subscriber details and itemised billing on an account, and if
- the only purposes for which this information can be obtained is 'for the purposes of preventing or detecting crime, or of preventing disorder'. It may be lawful to monitor internal 'Communications data', relevant to the authorities business if:
- it is on the authority's own telecommunications system, and
- the systems controller has made all reasonable effort to inform everyone that the communications may be intercepted, and
- the use of the monitoring is to investigate or detect unauthorised use of the telecommunications system, or
- determine whether they are personal communications, or other purpose permitted in Regulation 3 of the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000.

Private Information - is any information relating to a person's (see 2.2above) private or family life. For example if the investigation required an employee's home to be observed to determine their movements, then that surveillance would, probably gather private information, as would he surveillance if an individual selling counterfeit goods as the surveillance may provide information about the earnings that the person made from the sales.

Confidential Information - is information, which is:

- Matters subject to legal privilege
- Information held in confidence concerning an individual (living or dead) who can be identified from it and relating to physical or mental health or spiritual counselling
- Confidential Journalistic Material.

Confidential Information does not have any special protection under RIPA but particular care should be taken as such information may engage Article 6 of the European Convention on Human Rights (the right to a fair trial) as well as Article 8. Paragraph 3.5 also notes that legally privileged information obtained by surveillance is unlikely to be admissible as evidence in criminal proceedings. Therefore any such application should be made only in exceptional and compelling circumstances. All directed surveillance applications where confidential information is likely to be obtained, are required to be authorised by the Chief Executive.

6. Codes of Practice and Documentation

- Home Office's Statutory Code of Practice on Surveillance
- CCTV Code of Practice
- Acquisition and Disclosure of Communications Guidance
- RIPA Application and other forms
- Protection of Freedoms Act 2012 – changes to RIPA
- Protection of Freedoms Act 2012 – Magistrates' Court Guidance
- CHIS
- Investigatory Powers Commissioners Office

This page is intentionally left blank