**St. Helens Borough Council**

**Regulation of Investigatory Powers Act 2000**

**Policy Guidelines on the Use of Directed Surveillance**

**And Covert Human Intelligence Sources**

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides the statutory requirements which should be met in issuing authorisation to carry out surveillance. The Council carries out a wide range of enforcement functions. Some of these will from time to time involve covert surveillance, whether directed or using a human intelligence source in order to obtain evidence. The most common areas within the Council likely to engage in activities which require consideration under RIPA are those sections which regularly deal with enforcement issues, such as Trading Standards and Counter Fraud. Any department of the Council may, at some time, need to consider RIPA implications, and a general awareness within each department is necessary.

* 1. The Council recognises that its powers are wide-ranging and that they must be exercised in a reasonable, proportionate and sensitive manner. It is committed to observing the requirements of RIPA, both in practice and in spirit. The main purpose of RIPA is to ensure that investigatory powers are used in accordance with fundamental human rights and, in particular, the need to protect the right to an individual's privacy under Article 8 of the European Convention of Human Rights. It is important to remember, however, that RIPA provides not only protection for the rights of the individual, but also protection for the legitimate activities of the Council. As long as surveillance is both necessary and proportionate (as referred to later in this guideline) and takes place in accordance with both an authorisation and a judicial approval properly granted, then the Council and its officers have the protection of RIPA in relation to information obtained. Some surveillance activities do not need an authorisation/judicial approval and some enforcement actions are provided for by other legislation. Section 80 of RIPA specifically permits these latter actions to continue.
  2. The changes introduced by the Protection of Freedoms Act 2012 restrict the purposes for which local authorities may authorise directed surveillance. The power to undertake surveillance is limited to the prescribed purpose of preventing or detecting crime. The power is also limited to criminal offences that carry a custodial sentence of 6 months or more, unless the offence relates to under-age sales of alcohol and tobacco. It is therefore essential that consideration is given to the penalty attached to the criminal offence being investigated at the outset.

1.4 All directed surveillance or use of covert human intelligence sources carried out by officers of the Council, or by those acting on the Council's behalf, must be authorised in the first instance by one of the senior officers whose name and post title is listed in the Appendix. The authorisation will not take effect until a judicial approval has been granted. Officers who are more senior than those named may also authorise such surveillance in accordance with the provisions of the relevant legislation (currently the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, as amended). No-one directly involved in an investigation should act as Authorising Officer in relation to that investigation. The Council is required to obtain a judicial approval from the Magistrates Court before the internal authorisation can take effect. A judicial approval will also be required if authorisations are being renewed.

1.5 This policy is intended to be read in conjunction with the relevant Codes of Practice on Covert Surveillance and Property Interference and on the use of Covert Human Intelligence Sources issued by the Home Office. All officers of the Council, and those acting upon the Council’s behalf, who operate under RIPA, must operate in accordance with the Codes issued by the Home Office. The Codes of Practice are revised from time to time and are available on the internet at:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf>

And

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf>

1.6 This Policy is reviewed annually. Reports on the use of authorisations under RIPA are provided to the Council’s Audit & Governance Committee on an annual basis.

2. Implementation of RIPA

2.1 In accordance with its stated objective to use its powers in a reasonable manner, the Council expects its officers and those acting on its behalf to abide by the legislation and guidance issued. This is a fundamental requirement in itself, but in the context of RIPA, is also important to protect the rights of individuals to protect the Council and its officers and to ensure that the risk of legal challenge to our actions is minimised.

2.2 Whilst it would be trite to express the Council’s policy on RIPA as complying with the legislation and following the Codes of Practice, that is the policy in essence. In order to assist those people who are required to operate under the legislative requirements, however, the Council recognises the need to emphasise the fundamental points. It is hoped that by doing so, departments can ensure that their officers are able to operate to maximum effect, but with due respect to the rights of the individual. Departments will have differing operational activities which require procedures specific to their individual requirements. Each department will, therefore, have a procedure which covers its own needs, but each procedure must also be compliant with legislation and statutory guidance.

2.3 The Home Office has also issued a set of forms which deal with applications, reviews, renewals and cancellations of authorisations for directed surveillance and the use of a covert human intelligence source. These forms are revised from time to time and should be used by all departments when seeking authorisation. They are available on the internet at:

<https://www.gov.uk/government/collections/ripa-forms--2>

The Home Office has issued guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance. The guidance is available on the internet at

<https://www.gov.uk/guidance/surveillance-and-counter-terrorism>

And:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf>

A model application form for judicial approval is also available on the Home Office website at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/approval-order-form?view=Binary>

2.4 The Head of Legal & Democratic Services is the Council’s Senior Responsible Officer for RIPA matters. A copy of every authorisation, review, renewal or cancellation must be provided to the Head of Legal & Democratic Services who will maintain a central record in accordance with the Codes of Practice. Further details in respect of the central record are set out in paragraph 7. On occasion, Council officers may participate in joint enforcement operations with other organisations. In those cases where an external organisation deals with the RIPA application as the lead enforcement body, the relevant Council Service Manager will retain a copy of the internal RIPA authorisation and judicial approval for their records.

2.5 The Head of Legal & Democratic Services is also responsible for overseeing:

2.5.1 the integrity of the process in place within the authority for the management and

authorisation of CHIS and directed surveillance;

2.5.2 compliance with Part II of the 2000 Act and with the Codes of Practice;

2.5.3 oversight of reporting errors to the investigatory Powers Commissioner’s Office

(“IPCO”) and implementation of process to minimise repetition of errors

2.5.4 engagement with the Investigatory Powers Commissioner’s Office (“IPCO”) and

Inspectors when they conduct their inspections;

2.5.5 where necessary, overseeing the implementation of any post-inspection action

plans recommended by a Commissioner.

2.5.6 ensuring authorising officers are of an appropriate standard

3. The Fundamental Principles - Directed Surveillance

3.1 It is expected that Directed Surveillance will form the major part of any covert surveillance carried out by the Council. Directed surveillance is defined in Section 26 of RIPA and explained in the Code of Practice on the use of Covert Surveillance and Property Interference. It is defined as covert but not intrusive, and is undertaken for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation/operation) and otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable to seek an authorisation for carrying out surveillance.

* 1. Is the surveillance covert?

Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place. If activities are open and not hidden from the subjects of an investigation, the RIPA framework will not normally apply.

* 1. Is it for the purposes of a specific investigation or specific operation?

For example, are Town Hall CCTV cameras which are readily visible to anyone walking around the building, covered by RIPA? The answer is not if their usage is to monitor the general activities of what is happening in the car park. If that usage, however, changes, RIPA may apply. For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific operation.

* 1. Is it in such a manner that is likely to result in the obtaining of private information

about a person?

“Private information” is any information relating to a person’s private or family life. An

investigation that merely gathers intelligence about a person’s use of public spaces

and premises open to the public would not by itself usually be likely to result in the

obtaining of private information.

* 1. Examples of Surveillance

|  |  |
| --- | --- |
| Overt | - Police Officer or Dog Warden on patrol  - Signposted Town Centre CCTV cameras (in normal use)  - Most Test Purchases (where the purchaser behaves no differently from a member of the public) |
| Covert but not requiring authorisation | - CCTV cameras providing general traffic, crime or public safety information |
| Directed – must be subject to RIPA authorisation | - Undertaking surveillance activities, to establish whether an individual has fraudulently claimed a local taxation discount or exemption  - Test purchases where the purchaser has a hidden camera or recording device to record information which might include information about the private life of a shop-owner |
| Intrusive – **Council is not authorised to undertake this type of surveillance** | - Planting a listening or other device in a person’s home or in their private vehicle |

* 1. Use of Social Media in Investigations

The use of social media such as Facebook and Twitter may be used as an investigative tool to gather evidence in criminal investigations. However, personal information may be obtained by viewing a person’s social networking profile and/or creating a covert relationship with a member of the public. Repeat viewing of open profiles via social media in investigations may constitute directed surveillance. Consideration should therefore be given to the need for internal authorisation and a judicial approval. The following requirements aim to support the investigating officer in their enforcement duties and provide a framework of good practice:

* access to social networking sites by officers as part of an investigation should only take place with the prior agreement of the Service Manager
* a record of all social media/network accounts set up for the purpose of conducting investigations must be maintained by the relevant Section along with a record of usage
* access to social media sites must be proportionate to the alleged offence under investigation
* officers must not create a false identity in order to ‘befriend’ individuals on social networks without an internal RIPA authorisation and judicial approval
* officers viewing an individual’s profile on a social network should do so only once in order to obtain evidence to support or refute the alleged offence under investigation
* further viewing of open profiles on social networks to gather evidence or to monitor an individual’s status, must only take place once an internal RIPA authorisation and judicial approval has been granted
* officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity

The Council’s Social Media Investigations Procedure provides further detailed guidance in respect of conducting investigations.

3.7 The first point to emphasise is that any person who is unsure about whether to seek authorisation or unsure about whether to issue an authorisation, must seek immediate advice before acting. For those seeking authorisation, advice may initially be sought from their line manager, but it is always appropriate to seek the advice of a member of legal services. RIPA is a piece of legislation with serious human rights implications whenever it is engaged. The Council is concerned about an individual’s rights, but it is also concerned to guard against serious reputational risk. RIPA presents some difficult judgments which must be made from time to time. Whilst departments can and do operate their own procedures, this is an issue which affects the Council corporately and staff will never be criticised for seeking advice. The Code of Practice must be constantly referred to, but unfortunately it does not provide all the answers to every set of circumstances.

3.8 Written authorisations and judicial approvals should be obtained in advance of all operations. It can happen, however, that an investigation which was not intended to include covert surveillance, develops along these lines. In such circumstances, authorisations and judicial approvals must be sought immediately. It is expected that covert surveillance will be planned, that risk is assessed, and that insurance and health and safety requirements are considered. There is one exception to the requirement to obtain an authorisation/judicial approval when it would otherwise be necessary, which would take it outside the statutory definition of directed surveillance. That exception is in circumstances when, by way of an immediate response to events, the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of surveillance. However, this can only be relied upon due to force of circumstance and the nature in which the situation arose is likely to be the subject of close scrutiny. It is not an excuse for, or a solution to, poor investigatory practice. A detailed note of the circumstances must be made at the first opportunity and must be maintained on file.

3.9 The basic questions which anyone seeking an authorisation/judicial approval and anyone issuing an authorisation must first ask themselves, are:

(i) Is an authorisation **necessary** in this particular case to enable the Council to carry out the particular function required?

In this context, necessary, has a statutory meaning provided in Section 28 of RIPA. This lists the grounds which would meet the definition of necessary.

**The only ground upon which an officer of the Council can rely to seek/ issue an authorisation is for the purpose of preventing or detecting crime. The power to undertake directed surveillance is limited to offences that carry a custodial sentence of 6 months or more, unless the offence relates to under-age sales of alcohol and tobacco.**

(ii) Is authorising covert surveillance **proportionate** to what is sought to be achieved by carrying it out?

Whether an action is proportionate is a balanced judgment in relation to an individual’s rights, but issues which must be considered are whether the same result could be achieved by less intrusive means, whether action is excessive in terms of what it will achieve, that it can be carefully managed to meet the objectives and is not arbitrary, unfair or based on irrational considerations.

The Code of Practice states that the following elements of proportionality

should be considered:

* 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 target 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.

Whether an authorisation is proportionate should also be considered in terms of the risk of collateral intrusion.

(iii) Is there a risk of collateral intrusion?

This is intrusion into the privacy of people who are not directly the subjects of the action. Such intrusion must be considered in determining whether action is proportionate and steps should always be taken to minimise or avoid such intrusion.

3.10 The authorising officer must consider those crucial tests referred to in 3.9 before issuing an authorisation. Officers must direct their mind to the circumstances of the individual case with which they are dealing when completing the form. In relation to necessity, the authorising officer should consider whether there are available means by which the information can be obtained overtly. If so, there is no necessity for the authorisation. In relation to proportionality, the authorising officer will expect and require the applicant to give reasons why the covert activities are proportionate. The authorising officer, in exercising their judgment, will be aware of the type of surveillance proposed and the way in which it is proposed to conduct it. They will determine whether the reasons put forward by the applicant on proportionality are valid. In considering this issue, collateral intrusion is also a key determinant. The authorising officer must also continue to monitor the situation by reviewing the position, assessing the results of the authorisation, ensuring that the authorisation is cancelled in a timely manner and that documents are provided to the central record. They will set review dates and specific expiry dates in the authorisation (3 months from the date of the authorisation less 1 day). Authorisations should be reviewed within the 3-month period. If necessary, authorisations should be renewed in order to authorise a further period of time.

3.11 All involved in operating under RIPA must be aware that **the Council is not authorised to carry out Intrusive Surveillance** as defined in Section 26 RIPA, but which, for ease of reference, relates to covert surveillance carried out in relation to anything taking place in residential premises or a private vehicle and involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device.

3.12 If an authorisation is issued, as well as providing a copy to the Head of Legal & Democratic Services, it is also appropriate for the department to maintain its own record. This is important to enable authorisations to be kept under review and to be renewed or cancelled. Whilst written authorisations are valid for a period of three months from the date they took effect, it is poor practice to allow authorisations simply to run out. Every authorisation must be for the statutory period, normally three months for surveillance authorisations and twelve months for CHIS authorisations. For example, a surveillance authorisation granted at 14:10 hours on 9 June will expire on 8 September at 23:59 hours. Authorisations for juvenile CHIS last for one month. They should be kept under review and if the reason for the issue no longer exists, they should be cancelled and recorded as such. Every authorisation must be formally and promptly cancelled. A copy of the prescribed forms for review and cancellation should also be provided to the Head of Legal & Democratic Services for the central record.

3.13 Confidential Information

Information in relation to covert surveillance is, by its nature, sensitive. It may also

be confidential as outlined in the Code of Practice. For example, it may relate to

someone's physical or mental health. Particular care should be taken in cases where

the subject of the investigation might expect a high degree of privacy or where

confidential information is involved. Confidential information consists of matters

subject to Legal Privilege, confidential personal information or confidential journalistic

information. Departments should take appropriate steps to ensure the security of

confidential and sensitive information supporting action under RIPA. Where there is

a likelihood that knowledge of confidential information will be obtained, the

authorising officer must be the Chief Executive or, in their absence, a

Executive Director.

3.14 It is expected that those people directly involved in RIPA procedures are provided with appropriate training sufficient to meet their needs. Departments should consider this in preparing their Training and Development Plans.

4. Covert Human Intelligence Sources

4.1 The use of covert human intelligence sources (CHIS) is expected to be used far less frequently by the Council than directed surveillance. It is, however, of equal importance that the relevant Code of Practice is followed. It is also important that whoever is used as the source is appropriately protected and managed.

4.2 A person is a CHIS if

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within (b) or (c) below;

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

1. they covertly disclose information obtained by the use of such a relationship

or as a consequence of the existence of such a relationship.

RIPA is not intended to apply to circumstances where members of the public volunteer information as part of their civic duties.

4.3 All of the principles previously referred to in the section on directed surveillance are equally applicable here. For example, if in doubt about any aspect of the process, advice should be sought from legal services.

4.4 Anyone seeking an authorisation/judicial approval and anyone proposing to issue an authorisation must first answer, as for directed surveillance, whether the authorisation is **necessary**, as previously defined; whether it is **proportionate** and whether there will be any risk or collateral intrusion and how that can be minimised.

4.5 In addition, arrangements should be in place for the proper oversight and management of CHIS, including appointing individual officers for each CHIS, as defined by the 2000 Act, to ensure:

(a) that at all times an officer of the Council will have the day-to-day responsibility for dealing with the source, for the source’s security and welfare and for maintaining a record of the use made of the source. This officer will be known as the “handler”;

(b) that at all times another more senior officer of the Council will have the general oversight of the use of the source. This officer will be known as the “controller”.

(c) that relevant records will contain such particulars as are specified by the Secretary of State – the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725) set out these matters;

(d) that relevant records which disclose the identity of the source will not be available to persons, except to the extent that access is necessary.

4.6 The use of vulnerable individuals, who are or may be in need of social care services, and juveniles as CHIS, should only be authorised in exceptional circumstances and should be avoided, if possible. Authorisation must be by the Chief Executive or, in their absence, by a Executive Director. An authorisation which relates to a juvenile is subject to special safeguards issued by the Home Office. The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) set out the provisions to be satisfied. They include rules about parental consent, meetings, risk assessments and the duration of authorisations. Such an authorisation is valid for one month and not 12 months, as is usually the case. Legal advice must be sought in any such case.

4.7 Security and welfare of the source are extremely important and must be a prime consideration in the planning process. It should continue to be taken into account throughout use of the CHIS in any operation and, if necessary, after the close of the operation.

* 1. Tasking is the term used to refer to any assignment given to the CHIS. If the task required is to purchase products for testing, an authorisation may not necessarily be required. By contrast, developing a relationship with a person in the shop, for example to gain information about the seller’s suppliers of an illegal product, is likely to require an authorisation and a judicial approval as a CHIS. Each case must be considered on its individual circumstances and advice sought. If doubt remains about the requirements of an authorisation/judicial approval, it is preferable to seek one. The tests for whether one is issued will remain as previously outlined.

4.9 Consideration should be given to the risk that an informant may in reality be a CHIS even if not tasked to obtain information covertly by the Council. Care should be taken when an informant provides repeat information about a suspect or about a relative, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship. This may mean that the informant is in reality a CHIS, to whom a duty of care is owed if the information is then used. In the event, legal advice should be sought before acting on the information received from such an informant. The tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by the Council. It is possible therefore that a person will become engaged in the conduct of a CHIS without the Council inducing, asking or assisting the person to engage in that conduct.

4.10 Authorisations for the use of a CHIS must be provided to the Head of Legal & Democratic Services for the central record. Authorisations must be kept under review and, where necessary, renewed by the Magistrates Court or cancelled as previously indicated.

* 1. Despite the fact that it is likely to be used less frequently, officers who are likely to be

involved in seeking or issuing an authorisation/judicial approval for the use of a CHIS

should receive appropriate training, as should those officers whose responsibility it

will be to run or have the day-to-day overview of the operation/investigation.

1. Judicial Approval
   1. The authorisation will not take effect until judicial approval has been granted. A representative of Legal Services will present the application in the Magistrates Court with the assistance of the applicant (investigating officer).
   2. Approval can only be granted if the Magistrate is satisfied that:
2. there were reasonable grounds for the authorising officer approving the application to believe that the surveillance/CHIS was necessary and proportionate and that those grounds remain;
3. the authorising officer was of the correct seniority within the Council, i.e. a Director, Head of Service or Service Manager, in accordance with the 2010 Order;
4. the granting of the authorisation was for the prescribed purpose, i.e. preventing or detecting crime (and satisfies the serious offence test for directed surveillance).

5.3 **No activity permitted by the authorisation may be undertaken until a judicial**

**approval has been obtained.**

6. CCTV

Closed Circuit Television systems also have the potential to be used in planned and targeted surveillance operations. The normal use of overt CCTV systems would not normally fall within the parameters of RIPA, since members of the public are aware that such systems are in use. The Council has a separate CCTV Code of Practice, a partnership document with Merseyside Police to cover the operation of its system. Those involved with RIPA need to be aware, however, that if a CCTV system is used in a planned and targeted way, it may be necessary for authorisation for directed surveillance to be obtained. Senior officers in the CCTV suite must be provided with a copy of the authorisation and judicial approval (redacted, if necessary) and must only allow the CCTV system to be used for the purposes authorised. CCTV is also subject to controls under the Data Protection Act.

7. Central Record of Authorisations

The Central Record will be maintained by the Head of Legal & Democratic Services –

or their nominated representative. The Central Record is available for inspection by the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner’s Office, upon request. It will be retained for at least 3 years from the ending of the authorisation, following which the records will be destroyed.

The Central Record will contain the following information:

* the type and date of authorisation;
* the name and rank of the Authorising Officer;
* the unique reference number of the investigation or operation;
* the title of the investigation or operation, including a brief description and names of the subjects, if known;
* a copy of the judicial approval from the Magistrates Court to effect the authorisation;
* if the authorisation is renewed, when it was renewed by the Magistrates Court;
* whether the investigation or operation is likely to result in obtaining confidential information;
* the date the authorisation was cancelled.

8. Error Reporting

Errors are expected to be kept to a minimum by complying with both this policy and the aforementioned Codes of Practice. A “relevant error” occurs when a public authority fails to comply with a requirement imposed on it which is subject to review by a Judicial Commissioner – in these circumstances, the Council will notify the Investigatory Powers Commissioner of the error as soon as reasonably practicable and in any event no later than ten working days after it has been established that an error has occurred.

Where the error has occurred as a result of information provided by an outside source which has later proven to be incorrect (but the Council relied upon in good faith), this should still be reported to the Investigatory Powers Commissioner.

9. Conclusion

These policy guidelines are meant to act as an aide memoire to those involved with the operation of RIPA. They are not a substitute for regular referral to the Codes of Practice. No document can hope to cover every individual set of circumstances. The key message to those involved is, if in doubt, seek advice before action is taken.

Last Revision: April 2021

Last Reviewed: February 2022

**Appendix**

Tony Smith, Head of Regulation

Darrell Wilson, Chief Trading Standards Officer

Gordon Lee, Assistant Director – Revenues, Benefits & Contact Centre

(NB. Officers who are more senior than those named, and Executive Directors, are also prescribed for the purposes of the 2010 Order)