READING BOROUGH COUNCIL

Regulation of Investigatory Powers Act: Policy for Covert Surveillance, the use of a Covert Human Intelligence Source and the Acquisition of Communications Data

1 General Background

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a means for local authorities to authorise covert activities. It was introduced as a consequence of the Human Rights Act 1998, which enshrined the European Convention on Human Rights into UK law and came into effect on 2 October 2000. RIPA aims to ensure that public bodies respect the privacy of members of the public when carrying out their investigations and that there is an interference with privacy only where the law permits it and there is a clear public interest justification. RIPA ensures that covert investigations are conducted in such a way as to protect individuals' rights and act as a safeguard to protect council officers and the Council against any legal challenge.

The Investigatory Powers Commissioner's Office is responsible for regulating surveillance conducted by public authorities (a role previously undertaken by the Office of Surveillance Commissioners). This is done through a programme of inspections, followed by a report of the inspection findings. Inspections are usually conducted with little notice and local authorities are subject to inspection usually every third year. The Council was last inspected in January 2017.

This policy describes the legislation relating to covert law enforcement techniques and provides a broad overview of the procedures to be followed in using those techniques. Detailed advice for investigating and authorising officers can be found in the accompanying guidance document published on the Council's intranet.

Officers contemplating submitting a RIPA should consult with the Legal Department at the earliest opportunity.

2 Legislation

In 2012 the Protection of Freedoms Act came into force. Sections 37 and 38 of that Act amended the Regulation of Investigatory Powers Act 2000 to require that, where an Authorising Officer has granted an authorisation for the use of directed surveillance, for the use of a covert human intelligence source or for the acquisition of communications data, judicial approval will be required.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources (Amendment) Order 2012 amended local authorities use of RIPA. It restricted Authorising Officers from allowing the carrying out of directed surveillance unless it was for the purpose of preventing or detecting a criminal offence punishable by a maximum term of at least six months imprisonment or constitutes an offence under sections 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons act 1993 (sale of tobacco to children under 18 years old).

These provisions came into force on 1st November 2012.

Additionally, in complying with RIPA, officers must have full regard to the three Codes of Practice issued by the Home Office. These are The Covert Surveillance and Property Interference Code of Practice and the Covert Human Intelligence Sources Code of Practice, both published in August 2018; and the Acquisition and Disclosure of Communications Data Code of Practice issued in 2015. These codes can be found by accessing the following links:

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

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

https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

Although the Codes do not extend the Council's legal obligations under RIPA 2000 they are admissible as evidence in both criminal and civil proceedings. Further assistance is provided in the Procedures and Guidance document published by the Office of Surveillance Commissioners:

https://osc.independent.gov.uk/wp-content/uploads/2017/01/OSC-Procedures-Guidance-July-2016.pdf

For the purpose of this policy covert surveillance means the pre-planned covert watching or monitoring of a person or group of persons or the covert listening to a person or group of persons over a period of time which is carried out in a manner calculated to ensure that the persons subject to surveillance are unaware that it is, or maybe taking place, for the purpose of obtaining private information about them, other than as an immediate response to events.

Private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Information such as names, telephone numbers and address details are considered to be private. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public.

3 Types of Covert Surveillance

(i) Directed Surveillance

Directed Surveillance is defined in section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and undertaken:

(a) for the purposes of a specific investigation or operation;

(a) in such a manner as is likely to result in the obtaining of a private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(b) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

Directed surveillance involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a Trading Standards Officer on route to speak to a witness passes a side street and happens to see what appear to be goods being sold out of the back of a van. The officer parks up and hides around a corner to take photographs of the sales occurring. After 20 minutes the officer approaches the seller to enquire as to his actions. This would not require a RIPA authorisation as it is a response to immediate events.

(ii) Covert human intelligence sources

A person is a covert human intelligence source if:

He/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following bullet points

- He/she covertly uses such a relationship to obtain information or to provide access to any information to another person or

- He/she covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A purpose is "covert" in these circumstances if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

(iii) Communications Data

The 'who', 'when', and 'where' of a communication. It does not include the content; what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It does not include what they say or what data they pass on within a communication including text, audio and video.

(iv) Intrusive surveillance

Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that is:

(a) Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device

RBC is not permitted to authorise intrusive surveillance

It should be noted that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary.

4 Applications

Before authorisation is considered a full written application will be given to the authorising officer in the form approved by the Home Office. Copies of these are available within the Council but can be obtained from the Home Office website https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2

Consideration will be given that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve.

Particular consideration will be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance.

Consideration will be given to risk assessment.

Those carrying out the covert surveillance will inform the authorising officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way.

Consideration will be given to particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

Where RBC carries out surveillance on behalf of another Agency the tasking authority will be responsible for the authorisation.

Applications for surveillance should be in writing and should specify the information described in the approved forms referred to above and in the Codes, including;

- the nature of the surveillance;
- any premises or vehicles in relation to which the surveillance will take place;
- the identity of those to be the subject of the surveillance (where known);
- how the authorisation criteria are considered to be met; and
- Whether the operation or investigation is likely to lead to the acquisition of any religious/confidential material.

5 Authorisation

Before giving authorisation to the application the authorising officer will be satisfied that

- The surveillance is likely to be of value in connection with detection of crime, and is proportionate to the crime being investigated.

- The desired result of the Surveillance cannot reasonably be achieved by other means.

- The risks of collateral intrusion have been properly considered.

- Written authorisation will last for no longer than 3 months for directed surveillance and 12 months for a covert human intelligence source application.

- The authorisations is for an offence for which there is at least a maximum term of six months imprisonment

Legal Services hold a record of all Authorising Officers, only those listed are able to authorise RIPA applications. In the absence of any appropriate officer within the service applications may be dealt with by the Senior Responsible Officer (Assistant Director of Legal and Democratic Services).

6 Magistrates Hearing

Once the Authorising Officer has given their independent approval, the Investigating Officer will complete a Magistrates Approval Form and contact the Court to arrange a hearing. The Approval From can be obtained from the Home Office website https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa. The Investigating Officer will need to submit both the approval form and the application form for consideration by the Magistrate. The Investigating Officer will need to have the authority to appear before the Magistrate. Legal Services holds a record of such officers. It is advised that the Authorising Officer also attend the hearing to respond to any queries the Magistrate may have in relation to the approval.

7 Renewal

Applications for a renewal of an authorisation will include

- whether this is the first renewal or every occasion on which the warrant/authorisation has been renewed previously;

- the information listed as it applies at the time of the renewal;

- any significant changes to the information in the previous application for a warrant/authorisation;

- the content and value to the investigation of the product so far obtained under the surveillance;

- the results of periodic reviews of the operation by a senior officer.

Renewal forms can be obtained from the Home Office website:
https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2

Renewals will also need to be approved by a Magistrate.

8 Cancellation

On completion of the surveillance the authorisation must be cancelled by the authorising officer. Applications s must not be left to expire. Cancellation forms can be obtained from the Home Office website:
https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2

9 Use of the Internet to Carry out Surveillance

Officers can make use of the internet in the course of their enquiries. Often these enquiries are simple 'open source' enquiries and are unlikely to amount to either directed surveillance or the use of a covert human intelligence source. However, there are circumstances under which RIPA authorisation may be appropriate. Detailed guidance on this area can be found in the detailed guidance document produced for officers referred to under point 1.

For further information regarding this policy please contact the Data Protection Officer or the Information Officer in Legal Services.

10 Non RIPA Surveillance

As a result of the 2012 changes which led to a restriction in the use of RIPA by local authorities, surveillance may now be required which falls outside of RIPA (for example in the case of anti-social behaviour offences which do not attract a maximum custodial sentence of at least six months imprisonment). It is good practice to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the Senior Responsible Officer (SRO). The SRO will maintain an oversight of non RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The RIPA Monitoring Officer will maintain a central record of non RIPA surveillance.

As part of the process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed by the investigating officer. The form must be signed off by an authorising officer (Head of Service, Service Manager or Trading Standards Manager). A copy of the non RIPA surveillance application form is available from the Data Protection Officer or Information Officer in Legal Services or can be found on the intranet. The completed form should be forwarded to the Legal Department and details of the operation will be entered on to the central record by the RIPA co-ordinating officer.

Non RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance application form and authorised by the Head of Service in consultation with the Head

of Internal Audit. A central record of staff surveillance is also maintained by the RIPA Monitoring Officer.

Officers contemplating Non-RIPA surveillance should consult with the Legal Department at the earliest opportunity.

11 Complaints Procedures.

The Council's complaints procedure may be used for any complaint, regarding breach of this policy.

Contravention of the Data Protection Act 2018 may be reported to the Information Commissioners Office.

12 Records

- RBC will keep a central record of all surveillances authorised, renewed and cancelled. All completed forms should be forwarded to Legal Services.

- These records will be kept for 3 years from the end of the authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings they will be retained for a suitable further period.

- Where material is obtained which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation and there is no reason to believe it will be relevant to future investigations or criminal proceedings it will be destroyed immediately.

- The Data Protection Act will be complied with at all times.

- An annual report will be considered by Full Council providing Members with an update on the Council's use of RIPA during that year.

- The Council's Policy Committee will review this document on an annual basis to ensure that it remains fit for purpose.

October 2019