Brighton & Hove City Council

Corporate Policy & Guidance Document

On the use of covert surveillance

John Peerless
Head of Trading Standards
Telephone: 01273 292486
E-mail: john.peerless@brighton-hove.gov.uk

Version: November 2011

Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) grants considerable powers to the Council to undertake surveillance work to assist it in the detection of crime and prevention of fraud in respect of its various statutory and non-statutory activities.

The Act sets out in detail the type of surveillance work the Council may undertake, and the circumstances in which it may be undertaken. The Act also provides a regulatory framework, overseen by the Office of the Surveillance Commissioner with which the Council must comply. The Commissioner also publishes codes of practice (available on the Home Office website), which the Council follows in implementing the RIPA framework.

The Council has various duties in connection with the prevention and detection of crime. These include environmental enforcement work, detection of benefit fraud, and the investigation of allegations of fraud against staff or contractors. On occasion it will be necessary to undertake surveillance work in order to either gather evidence to support a prosecution, or to confirm that there are no grounds for further action. Surveillance activities normally involve following people, or using CCTV cameras, or still or time-lapse photography to observe people.

Surveillance is controlled by a system of authorisation, which requires a senior officer to consider the purposes for which surveillance is to be undertaken, and the arrangements for ensuing that it is undertaken in accordance with the requirements of Guidance issued by the Office of the Surveillance Commissioner.

Training is offered to staff whose work is likely to bring them into contact with the RIPA regime.

Policy Statement

The Council supports the statutory framework for surveillance as a means of safe-guarding the legitimate interests of individuals, whilst ensuring that there is proper investigation of cases.

The Council follows the guidance issued by the Office of the Surveillance Commissioner. The Guidance contains 6 points:

Ensure that relevant officers understand the scope of RIPA in relation to their work:
Those staff whose jobs are likely to involve surveillance work should be trained on the Act and its implications. The training serves two purposes, first in ensuring that they understand the procedures and safeguards within the system, and, to minimise the risk that staff will attempt to undertake investigation using methods incompatible with the requirements of RIPA.

Ensure that consideration is given to identifying the activities to which RIPA may apply:
For local authorities this means investigatory work involved in the prevention and detection of crime. The services that potentially will be involved in such work are:
Benefits Investigations,
Internal Audit,
Waste Management
Trading Standards
Adult Social Care, and
Children Services

This, however, is not an exhaustive list.

Develop a local policy on the use of RIPA:
The Council's policy is that RIPA should only be used when it affords the most effective way of gathering evidence in respect of an allegation. However, it is not the case that RIPA will only be used when there is no other way of gathering information, since in some instances, the alternatives may be too costly in terms of time and money. However, careful consideration must always be given to alternative methods before seeking authorisation under the RIPA regime, in order to ensure that the use of surveillance is a proportionate response to the circumstances of the case.

Identify individual officers who will be able to authorise the use of the powers:
Authorisations should be signed by the relevant Head of Delivery Unit or Head of Service.

Establish procedures by which the powers will be authorised:
This Guidance sets out the framework for obtaining authorisations for surveillance.

Ensure training is provided to officers who will use the powers, particularly in relation to the issues of proportionality and necessity:
All staff who may use the RIPA framework should receive training. Training requirements will be considered as part of individual performance review, and will be

reviewed periodically by the Director of Finance & Governance in relation to monitoring of authorisations.

Guidance for officers

Types of surveillance

'Surveillance' includes

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

Surveillance can be overt or covert.

Overt Surveillance

Most surveillance activity will be done overtly, that is, there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a Neighbourhood Warden walking through the estate).

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

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

Directed Surveillance is surveillance which: -

- Is covert; and
- Is not intrusive surveillance;
- Is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- It is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation).

Intrusive Surveillance

If the surveillance involves anything taking place in residential premises or a vehicle and involves the presence of a person or surveillance device on or in the premises or vehicle, then RIPA imposes very strict limitations.

Such surveillance is Intrusive Surveillance and is not available to local authorities.

No officer of the Council is permitted to grant an authorisation for Intrusive Surveillance and if you consider the surveillance you propose might be intrusive you must seek advice from the Head of Trading Standards.

Covert Human Intelligence Sources (CHIS)

There are specific rules governing the use of CHIS in the legislation and codes of guidance.

The Council does not as a rule make use of CHIS. But if any officer considers that the use of CHIS might be appropriate in a particular case, the matter should be referred to the Head of Trading Standards.

If it appears that the use of CHIS is proportionate authorisation must be obtained from the Chief Executive who should then give consideration to the additional health and safety safeguards.

Private Information

Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person.

Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

Directed (or covert) surveillance should only be undertaken where it is necessary or expedient for the proper discharge of the Council's duties.

This does not mean that it is a last resort, in some cases, the most effective and efficient means of gathering information will be through directed surveillance. However, the use of surveillance must be proportionate to the matter being investigated. This means that the nature of the case, and the issues raised in terms of resolving an allegation, or gathering evidence must be set against the potential for intrusion into the personal life of the person under surveillance.

When might the Council undertake covert surveillance?

The Council is involved in every day functions of law enforcement. For example Benefit fraud investigation officers might covertly observe a benefit claimant suspected of fraud.

What safeguards must the Council observe before undertaking surveillance of any sort?

The Council has to be satisfied that the surveillance is undertaken in connection with a statutory function with which the Council is charged.

All covert surveillance must meet the two tests of necessity and proportionality. The Council must ensure it meets its obligations under Article 8 of the Convention on Human Rights, i.e. to protect the right of the individual and to have respect for private and family life.

Covert surveillance by its very nature interferes with this right. It is acceptable to so interfere with Article 8 rights if it is to achieve an objective that is recognised as being of public importance (in this instance the prevention and/or detection of crime), and the means used (in this case covert surveillance), are necessary in order to achieve that objective in the circumstances of the particular case.

For this reason, the procedure used for authorisation of RIPA surveillance requires that reasons are set out which demonstrate both the objective, and the necessity and proportionality of using covert surveillance.

The surveillance must be properly authorised and lawful.

What does the Regulation of Investigatory Powers Act 2000 say?

The Act regulates the use of investigatory powers that are to be externally supervised by Surveillance Commissioners, and it was passed to ensure that law enforcement and other operations have been properly issued and any person involved in investigations person acts in accordance with that authorisation. This is important because:

A person acting in accordance with a duly issued authorisation will be protected from civil liability, and

If the Council is involved in any proceedings before the Court the Council will be able to show that it has acted lawfully and that it has gathered evidence properly, and an individual's right to a private and family life has not been interfered with without due consideration of whether that interference was necessary and proportionate.

How is an application for authorisation made?

The applicant must notify the PA to the Head of Environmental Health & licensing that directed surveillance is being considered and obtain a unique reference number (URN).

They must complete an application for authorisation to carry out Directed Surveillance on the standard Home Office forms. These are to be found on their website.

Once drafted, the form must be submitted to the 'gatekeeper'. They will review all applications and ensure that

- The applicant has obtained a Unique reference Number (URN), (obtained from the PA to the Head of Environmental Health & Licensing)
- The correct form has been used and correctly completed
- The application contains sufficient detail and supporting information
- The application complies with the necessity and proportionality requirements
- Their comments are recorded and maintained, and where necessary
- They provide feedback to the applicant.
- Pass to the relevant Authorising Officer for authorisation

If there is a genuine urgency, then oral authorisation may be given, which must be followed up with written authorisation within 72 hours. There are likely to be very few such instances.

Grounds for Authorisation

The need for necessity

The Authorising Officer must record why they are satisfied that there is a necessity to use covert surveillance in the proposed operation. In order to be so satisfied there must be a serious crime that needs to be prevented or detected before an authorisation should be granted.

In this context includes consideration as to whether the information sought could be obtained by other less invasive means, and that those methods have been explored and been unsuccessful or could have compromised the investigation.

Serious Crime

With the exception of the work of Trading Standards to tackle the sale of age restricted products, the Codes now limit the use of covert surveillance to tackling serious crime.

This has been identified as any offence for which the offender could be imprisoned for 6 months or more. This will automatically restrict the use of surveillance activity under this frame work by a number of our services as the offences that they investigate do not meet the above criteria, or they do not deal with criminal matters.

An analysis of relevant offences indicates that covert surveillance may therefore be used by Housing Benefit (fraud), Trading Standards (various offences including Consumer Protection from Unfair Trading Regulations and door step crime), Waste Enforcement (fly tipping), Fraud against the Council and Child protection and Adult safe-guarding issues.

The need for proportionality

Deciding whether the activity is proportionate includes balancing the right to privacy against the seriousness of the offence being investigated. Consideration must be given as to whether the activity could be seen as excessive.

The Authorising Officer must also record why they have reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate to what it seeks to achieve.

A potential model answer would make it clear that the 4 elements of proportionality had been fully considered.

- Balancing the size and scope of the operation against the gravity and extent of the perceived mischief
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
- That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result and,
- Evidencing what other methods had been considered and why they were not implemented.

How long will the authorisation last?

The written authorisation will cease to have effect (unless renewed) at the end of a period of 3 months beginning with the date on which it took effect.

Exceptionally, an oral authorisation may be given in cases of urgent necessity, in which case the detail referred to above should be recorded in writing as soon as reasonably practicable. Such authorisations will cease to have effect after 72 hours beginning with the time when the authorisation was granted.

When approving the surveillance, the Authorising Officer will set a review date which must be as soon as reasonably practical and no longer than 28 days after the date of authorisation, and on which the Authorising Officer will personally review the authorisation. This helps to ensure that authorisations are up to date.

Cancellations and renewals

All authorisations automatically cease after 3 months. However, authorisations should be cancelled as soon as the need for the authorisation has passed, notwithstanding the review date on the form.

Use of CCTV

CCTV is not normally covered by RIPA. Areas where CCTV operates should be advertised by placing appropriate notices. This is because surveillance which is “general”, or overt, such as CCTV surveillance in a reception area, is not subject to RIPA.

Where CCTV is intentionally used to track an individual or group of individuals as part of a surveillance exercise, then RIPA will apply. Staff in the Police CCTV Control Room will always request a copy of the authorisation.

CCTV tapes arising from surveillance must be retained in a secure store within the CCTV area until handed over to the case officer dealing with the case.

What records must be kept?

The following records must be kept:

- A copy of the application for authorisation.
- A copy of the authorisation.
- A record of the period over which the surveillance is taking or has taken place (including any significant suspensions of coverage).
- A record of the result of periodic reviews of the authorisation.
- A copy of any renewal authorisation, together with the supporting documentation when the renewal was requested.
- A copy of the cancellation

Copies of all documents must be submitted to the PA to the Head of Environmental Health & Licensing for inclusion in the Central Record.

Oversight

Senior Responsible Officer

The revised Code of Practice recommends that each public authority appoints a Senior Responsible Officer (SRO). A recent review of those codes indicates that the SRO should be a member of the corporate management Team and for the purposes of this policy the Director of Finance and Resources has been so delegated.

The SRO is responsible for

- The integrity of the process in place within the public authority to authorise directed surveillance;
- Compliance with the relevant Acts and Codes of Practice; engagement with the Commissioners and Inspectors when they conduct their inspections, and where necessary,
- Over seeing the implementation of any post inspection action plans recommended or approved by a Commissioner.
- Ensuring that all authorising officers are of an appropriate standard and competence.

Councillor scrutiny

Changes in the legislation gave a formal scrutiny role to Councillors and Cabinet now review the use of RIPA on a quarterly basis and the Policy on an annual basis.

Office of the Surveillance Commissioner

The Chief Surveillance Commissioner and Surveillance Commissioners together with their Inspectors have been appointed to provide independent oversight of the use of the powers contained in Part II of RIPA.

They will inspect the Council from time to time to ensure that the Council is complying with the Act. In addition, the Act establishes an independent tribunal. This tribunal has full powers to investigate and decide any case where a person complains about the conduct of the Council in exercising its powers carrying out surveillance.

Training

All officers whose work involves, or is likely to involve the use of the RIPA regime should receive training once every three years. Training should be by way of attendance on a course run by someone with expertise in the use of RIPA. The issue of training should be included in the annual appraisal for staff in relevant services.

The PA to the Head of Environmental Health & Licensing maintains records of RIPA training.

In addition, there should be regular updates at team meetings on the use of RIPA.

Forms

Copies of the following forms are available from the Home Office website:

Application for authority for Directed Surveillance

Application for renewal of Directed Surveillance Authority

Cancellation of Directed Surveillance

Authorising Officers

The following officers may authorise RIPA surveillance:
Head of Internal Audit & Risk
Head of Revenue & Benefits
Head of Adult Assessment
Head of Children & Families
Head of City Infrastructure
Head of Trading Standards

Gatekeeper

This person(s) should maintain a high level of knowledge of RIPA and a good understanding of the council services that use covert surveillance as an investigation tool. They would provide advice to applicants and their managers to ensure that the application is completed correctly and that the necessity and proportionality rules are comprehensively addressed.

The following officers will perform the gatekeeper role:
Head of Trading Standards
Principal Trading Standards Officer

Access to Communications Data

Local authority employees (except Housing Benefit Officers) are no longer able to use their powers under relevant legislation and the exemption under the Data Protection Act 1998 to obtain communications data.

Local authorities may only access Customer Data or Service Data. **They cannot access 'traffic data'.**

Customer data (Subscriber)

Customer data is the most basic information about users of communication services.

It includes:-

- The name of the customer
- Addresses for billing, etc.
- Contact telephone numbers
- Abstract personal records provided by the customer (e.g. demographic information or sign up data)
- Account information (bill payment arrangements, bank or credit/debit card details
- Services subscribed to.

Service Data (Service user)

This relates to the use of the Service Provider services by the customer, and includes:-

- Periods during which the customer used the service
- Information about the provision and use of forwarding and re-direction services
- Itemised records of telephone calls, internet connections, etc
- Connection, disconnect and re-connection
- Provision of conference calls, messaging services, etc
- Records of postal items, etc
- Top-up details for pre-pay mobile phones.

Traffic Data

This is data about the communication. It relates to data generated or acquired by the Service Provider in delivering or fulfilling the service**.**

Such disclosure by Communication Service Providers will now only be permitted if a notice to obtain and disclose (or in certain circumstances an authorisation for an officer to obtain it themselves) has been issued by a 'Designated person'.

Authorities have to nominate Single Point of Contact and those person(s) must have undertaken accredited training. The National Anti Fraud Network (NAFN) whose southern team is hosted by the Council has been accredited by the Home Office and is the nominated SPOC for the Council.

The 'Designated Persons' within the Council is now limited to the Head of Trading Standards

.