APPENDIX E

Internal Audit

The Policy and Code of Practice of The Regulation of Investigatory Powers Act 2000 (RIPA)

17 January 2012

Purpose

London Borough of Barking & Dagenham, "the Council" considers the RIPA Policy as being necessary to the proper conduct of crime prevention activities that involve use of covert directed surveillance. The Council has compiled a RIPA Code of Practice in accordance with the RIPA Act 2000 detailing the procedures necessary to comply with legislative requirements.

Staff found to have breached the RIPA Act and the Council's Code of Practice are deemed to have breached the Council's staff Code of Conduct and liable to disciplinary action.

Related Documents

This policy sets out the Council's approach to covert surveillance and the use of covert human intelligence sources. In particular, it details the checks and balances in place to ensure that any use of covert techniques is lawful, necessary and proportionate.

Who is Governed by this Policy & Strategy?

The RIPA Policy covers all council staff and those working on behalf of the Council who are engaged in crime prevention and detection activities which involve the use of surveillance.

Executive Summary

Local authorities can undertake surveillance and access communications data under the framework of the Regulation of Investigatory Powers Act 2000 (RIPA) allowing local authorities to use directed surveillance and covert human intelligence sources in order to prevent or detect crime or disorder in connection with their statutory functions.

These rules set high standards for all public authorities that use these powers to undertake a range of enforcement functions to ensure they can keep the public safe and bring criminals to justice, whilst protecting individuals' rights to privacy.

The London Borough of Barking & Dagenham has a strategy for tackling fraud and corruption, which covers reporting and investigation. In some circumstances the borough may wish to use surveillance techniques. RIPA defines the types of surveillance activities, which must be subject to a formal written procedure for both authorisation and conduct.

This policy describes the Council's procedures for use of RIPA powers to be compliant with the RIPA Act 2000 and associated Code of Practice.

In line with recent revised Code of Practice issued by Central Government and pending introduction of revised legislation contained within the Protection of Freedoms Bill, LBBD will only use covert surveillance where it is proportionate and necessary to do so, and only in the investigation of serious criminal offences.

Contents

The Regulation of Investigatory Powers Act Policy

The Regulation of Investigatory Powers Act 2000 (RIPA) is concerned with the regulation of surveillance by public authorities in the conduct of their legitimate business. Surveillance is an unavoidable part of modern public life, but has not until now been the subject of formal statutory control. RIPA was enacted to regularise that position and to ensure that, in conducting surveillance, public authorities have regard to The Human Rights Act 1998 and to Article 8 of the European Convention on Human Rights – the right to a private and family life.

The use of surveillance is an interference with rights protected by Article 8 of the European Convention on Human Rights and is prima facie a violation of those rights unless the interference is in accordance with the law, is in pursuit of one or more of the legitimate aims established by Article 8(2) and is "necessary in a democratic society"

The Council is defined as a Public Authority to which the Act applies by virtue of Section 1 of the Local Government Act 1999. The forms of surveillance that it is entitled to authorise are covert directed surveillance and the use of Covert Human Intelligence Sources (informants), known as CHIS

The London Borough of Barking & Dagenham has approved a strategy for tackling fraud and corruption, which covers reporting and investigation. However, in some circumstances the borough may wish to use surveillance techniques. RIPA defines categories of Public Authorities regulated by the Act together with acts of surveillance, which must be subject to a formal written procedure for both authorisation and conduct.

What is the Regulations of Investigatory Powers Act 2000 (RIPA) ?

The Regulation of Investigatory Powers Act regulates the work of the Council in the key areas of enforcement and prosecutions, and provides a legal framework for the Council to carry out surveillance which is not intrusive and is undertaken for the purposes of a specific investigation or a specific operation in such a manner as is likely to result in the obtaining of private information about a person. ***This is known as Directed Surveillance***.

The Act also regulates the Council's use of undercover officers or informants to obtain information. Under the Act they are referred to as Covert Human Intelligence Sources ('CHIS').

It is necessary for the Council to have a policy in order to describe and record the way in which the Authority complies with the Regulation of Investigatory Powers Act.

Regulations of Investigatory Powers Act 2000

The covert surveillance regulated by the RIPA 2000 (the Act) and covered by the Code of Practice is divided into two categories: intrusive surveillance and directed surveillance. Authorisation under the Act gives lawful authority to carry out certain types of covert surveillance.

What is not intended to be covered by the Act?

- General observations such as monitoring the crowd to maintain public safety and prevent disorder
- Trading standards or HM Customs & Excise officers covertly observing and then visiting a shop as part of their enforcement function
- General observations using equipment such as binoculars or cameras where this does not involve systematic surveillance of an individual
- Open use of CCTV surveillance systems where members of the public are aware that such systems are in use, for their own protection, and to prevent crime

Surveillance

What is Covert Surveillance? - Surveillance carried out in a manner calculated to ensure that the person(s) being surveyed are unaware that they are being observed.

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

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

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

(c) 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 for an authorisation under this Part to be sought for the carrying out of the surveillance.

What is Private Information? - Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.

Examples of Directed Surveillance - 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.

Examples of Surveillance which is not Direct Surveillance - 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 plain-clothes police officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol.

Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as "intrusive surveillance" and authorisation for this will not be given for a Local Authority.

Directed surveillance does not include entry on or interference with property or wireless telegraphy. These activities are subject to a separate regime or authorisation and again such authorisation will not be given to a Local Authority.

What is Intrusive Surveillance? - It is defined as covert surveillance that:

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

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

Where surveillance is carried out in relation to anything taking place on any premises or in any vehicle by means of a device which is not actually on the premises or in the vehicle, it is not intrusive unless the device 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. Therefore, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises would not be considered as intrusive surveillance.

Residential premises can include a house, a yacht, a railway arch, makeshift shelter, hotel rooms, bedrooms in barracks and prison cells but not any common area to which a person is allowed access in connection with his or her occupation of such accommodation e.g. a hotel lounge.

A private vehicle is defined as any vehicle which is used primarily for the private purpose of the person who owns it, it does not include taxis.

The Council cannot be authorised to carry out intrusive surveillance.

What if the Council works with another agency? - In cases where one agency is acting on behalf of another, it is normally for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by the Council on behalf of the police, authorisations would be sought by the police and granted by the appropriate authorising officer within the police force.

The London Borough of Barking & Dagenham Code of Practice

The Government provides full guidance on the use of covert surveillance by public authorities under Part II of the 2000 Act in its **Code of Practice** and is available on the Council Intranet Site

How does RIPA affect the Council's activities?

Types of Surveillance

Surveillance of Council property to detect anti-social behaviour.

Where the Council quite openly sets up CCTV cameras to monitor common or public areas of Council owned housing estates then the surveillance would not be covert and therefore would not fall under the act.

If however any surveillance was covert then as long as it did not collect private information about an individual(s) then authorisation should be sought under the following purpose: for the purposes of preventing and detecting crime.

If the surveillance collected private information about an individual e.g. watched someone coming in and out of their home, then such an individual would probably be able to argue that the Council had been in breach Article 8 of the Human Rights Act – the right to respect for his private and family life, home and correspondence. In such a situation, authorisation should be sought. Although the obtaining of authorisation would not in itself prevent an individual bringing a claim for breach of Article 8, because Article 8 does not confer an absolute right, the Council may be able to defend the claim by demonstrating that an evaluation of the necessity and proportionality of the need for the surveillance had been carried out by the Authorising Officer.

Surveillance of Council employees in the workplace.

Again, open surveillance would not fall under RIPA as long as staff were consulted and knew where the cameras were. If the cameras were introduced in a high handed way, without consultation then an employee could have a claim for constructive dismissal in that the sudden introduction of unreasonable filming constituted a breach of contract. The lawfulness will depend on the nature and degree of the filming e.g. installing a camera in a stationery cupboard where there have been many thefts as opposed to the installing of a video camera with sound recording in the coffee break area.

If the Council wishes to covertly film officers then as long as the purpose for the surveillance falls under the listed purpose: to prevent and detect crime – then authorisation should be sought. However, the filming could still be questionable employment practice for the reason set out above – and may lead to a claim for constructive dismissal. Considerations of privacy can also apply to a person's life at work, so a Human Rights Claim could also be made, and possibly defended in the same manner as above – namely by the obtaining of authorisation.

Surveillance of employees who are suspected of 'moonlighting' or malingering

There is no requirement on the part of a public authority to obtain an authorisation for a covert surveillance operation to monitor activities in this regard and the decision not to obtain an authorisation would not, of itself, make an action unlawful. However, equivalent consideration should be given to such actions which will make the action less vulnerable to challenge under the

Human Rights Act 1998. Section 71 of the Act places the Council under a mandatory duty to have regard to the provisions of the code.

Carrying out surveillance of the sort would necessarily involve the collection of private information and would leave the Council open to a claim for a breach of Article 8 of the Human Rights Act.

As above, it could also leave the Council open to a claim for constructive dismissal.

Furthermore, where an officer follows an individual for a significant length of time, there is also a risk that this work will be regarded as a form of stalking in breach of the Protection from Harassment Act 1997.

If an employee is suspected of claiming statutory sick pay as well as working then the matter would be a fraud against the Benefits Agency who could be authorised to conduct their own surveillance.

What of the recording of telephone conversations?

The Council is not able to covertly record telephone conversations but the use of a surveillance device should not be ruled out simply because it may incidentally pick up one end of a telephone conversation, and such product can be treated as having been lawfully obtained. Further, where one party to the conversation consents, and where the surveillance is authorised, the interception is treated as directed surveillance. For example, a person may consent to the recording of a telephone conversation sent by or to him.

However, such an authorisation cannot be used as a means of deploying recording equipment without obtaining the proper authorisation. If any other recording equipment is to be used, other than in the presence of the person who has consented to the recording then the surveillance should not continue.

Covert Human Intelligence Sources (CHIS)

A person is a covert human intelligence source if he/she develops a relationship with another person in order to covertly obtain information or to provide access to information to a third party or to covertly disclose information obtained by the use of such a relationship and the other person is unaware that the purpose of the relationship is one of the above. The use of a CHIS must be recorded by the authorising officer and approved by the Lead Officer.

The Council does not at present utilise CHIS. Any consideration of such use can only be considered with prior discussion with the Divisional Director of Assurance & Risk and/or Head of Legal.

For Directed Surveillance

Covert directed surveillance means surveillance so carried out that the persons subject to the surveillance are unaware that it is or may be taking place. Surveillance is directed if it is covert, but not intrusive, and is undertaken for the purposes of a specific investigation, in such a manner to obtain private information about a person, and otherwise than by way of an immediate response to events where authorisation could not be sought.

Directed surveillance will only be carried out with the express authority of the authorising officer.

Authorisation

In a Public Authority such as the council, only officers of the rank of Deputy Chief Officer or their nominated deputy and above may be designated as Authorising Officers for the purposes of the Act. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority

Covert surveillance that is properly authorised will, as long as it is carried out in accordance with the terms of the authorisation, be legitimate. The authorisation will provide a defence to a challenge under the Human Rights Act

Investigations requiring the use of covert directed surveillance or covert human intelligence sources may only be undertaken by officers of the Corporate Anti-Fraud Team (CAFT) or by specialist investigators who are professionally qualified and approved, engaged by the Authority

The Council will appoint authorising officers of suitable seniority to grant surveillance authorisations for individual incidents.

An authorisation for directed surveillance may be granted by the authorising officer who will be the Assistant Chief Officer responsible for the management of an investigation or anyone senior to him/her. The Authorising Officer must believe that the authorisation is necessary on the following grounds: **for the purposes of preventing and detecting crime or of preventing disorder.**

When considering the giving of authorisation the authorising officer must also consider the following:

- That the surveillance is proportionate to what it seeks to achieve
- Whether or not the privacy of persons other than the subject(s) of surveillance will be interfered, if so then it may even be necessary to consider whether a separate authorisation is required
- Particular consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his/her home, or where there are special sensitivities

How do you obtain an Authorisation? - Authorisations must be given in writing by an authorising officer and will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time at which it took effect.

In urgent cases where it is not possible for the requesting officer to complete the form there remains a requirement for the Authorising Officer to be consulted in order for an oral authorisation to be granted.

1. Oral authorisation in an urgent situation may only be granted for a maximum of 72 hours. A written application for Authorisation must be completed as soon as possible following ‘the oral grant and in any case within the 72 hour period’.

2. A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.

In cases of emergency, the investigating officer will obtain authority from either the authorising officer or their deputy by telephone, with the authorisation being confirmed in writing as soon as possible thereafter.

A central record of authorisations will be kept centrally by the Divisional Director of Assurance & Risk and will be monitored and reviewed on a regular basis by the Monitoring Officer. The records will be confidential.

Any request received from external authorised agencies, such as the police or security services either to disclose communications data, e.g. Billing information, e-mail addresses, etc., or to unlock encrypted data or provide the key to unlock encrypted data, will be referred to the Divisional Director of Assurance & Risk who will have the power to authorise such requests in consultation with the Head of Legal Services.

Authorising Officers must also assess the extent to which confidential information about the subject will come into the Authority's possession as a result of the investigation. Such information may be relevant to the investigation but protected for example as a result of legal professional privilege or it may be irrelevant but sensitive information for example medical records. Deliberately obtaining (or the use of) confidential information may only be authorised by the Chief Executive as laid down in Schedule 2 of the RIPA Act 2000.

Finally, the Authorising Officer should give due consideration to the impact on the community of the use of covert surveillance methods. In particular the officer should have regard to community confidence. The officer should consider if the circumstances of the investigation were to become public, what the reaction of the community is likely to be and whether and to what extent the Authority would be able to justify the use of its chosen methods.

All requests for an authorisation to conduct covert surveillance should be submitted by the appropriate officer to the Authorising Officer in writing using the forms attached to this policy note as updated from time to time by the Coordinating Officer, and completed in compliance with the written guidance.

Whatever the nature of the decision taken by the Authorising Officer, the decision should be confirmed in writing with reasons for the decision. Authorisations should be regularly reviewed in compliance with the legislation and the reasons for extending or terminating them should be recorded in writing.

Authorisations must not be allowed to expire. Authorisations must be reviewed regularly or cancelled after surveillance has been completed and put onto central records.

Surveillance should be carried out according to written procedures, adhering to good practice and health and safety conditions. Advice may be taken from the Divisional Director of Assurance & Risk and Corporate Anti-Fraud Team. All officers involved in applying for, authorising or undertaking surveillance will understand the legal requirements set out in RIPA and the Code of Practice. They will personally take responsibility for ensuring the propriety of their involvement. All authorisations, notebooks, surveillance logs and other ancillary documentation that relates to surveillance will be maintained to the required standards and retained for three years. All documentation will be volunteered for any management or regulatory inspection on demand.

Wilful disregard of any part of the RIPA Code of Practice or of internal procedures shall be a breach of the Code of Conduct for council officers and will be dealt with accordingly.

Further Support, Tools & Guidance

Link to the websites for the Surveillance Commissioner, the Home Office and the Office for the Public Sector Information can be found here:

- http://www.surveillancecommissioners.gov.uk/
- http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1
- http://www.surveillancecommissioners.gov.uk/about_covert.html

Designated RIPA Coordinator and Authorised Officers

Designated RIPA Coordinator and Authorised officers can be found here:
http://lbbd/resources/authorising-officers.htm

RIPA forms

Can be accessed here:

http://lbbd/corporate-finance/ripa-2000.htm

For further information, please access www.surveillancecommissioners.gov.uk

The latest version of the RIPA Policy and all of our documents can be obtained from either contacting the Group Manager – Internal Audit directly or by visiting our intranet pages:

Hyperlink?

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

david.greenfield@lbbd.gov.uk