Brighton & Hove City Council

Corporate Policy & Procedures Document

On

The Regulation of Investigatory Powers Act 2000

(RIPA)

John Peerless
Head of Trading Standards
Telephone: 01273 292486
Fax: 01273 292524
E-mail: john.peerless@brighton-hove.gov.uk

Version: June 2007

Contents Page

The Regulation of Regulatory Powers Act 2000 refers to 'Designated Officers'. For ease of understanding and application this document refers to 'Authorised Officers'.

Introduction

This document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office's Code of Practices for Directed Surveillance and Covert Human Intelligence Sources (CHIS) and Accessing Communications data.

The authoritative position on RIPA is the Act itself and any Officer who is unsure about any aspect of this document should contact the Head of Trading Standards or the Head of Law, for advice and assistance.

This document has been approved by the Policy & Resources Committee and is on 'The Wave'.

The Head of Trading Standards will maintain the Central Register of all authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorised Officer to ensure that relevant form is submitted within 1 week of its completion.

This document will be subject to a 6 monthly review by the Head of Trading Standards.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlap with the Council's Information Technology policies and guidance, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its draft Code Of Practice. RIPA forms should only be used where **relevant** and they will only be **relevant** where the **criteria** listed are fully met.

Policy Statement

The Council takes its statutory responsibilities seriously and will at all times act in accordance with the law and takes necessary and proportionate action in these types of matters. In that regard the Head of Trading Standards is duly authorised to keep this document up to date and amend, delete, add or substitute relevant provisions, as necessary. For administrative and operational effectiveness, the Head of Trading Standards is authorised to add or substitute Authorised Officers with the agreement of the relevant Director.

It is this Council's Policy that

- All covert surveillance exercises conducted by the Council should comply with the requirements of RIPA
- An Authorisation will only be valid if signed by two designated officers.
- Authorising 'Access to Communications data' will be restricted to the Head of Trading Standards and the Head of Operations, Public Safety

Authorised Officers Responsibilities

It is essential that Senior Managers and Authorised Officers take personal responsibility for the effective and efficient operation of this document.

Relevant Directors should ensure that sufficient numbers of Authorised Officers receive suitable training on RIPA and this document, and that they are competent.

It will be the responsibility of those Authorised Officers to ensure that relevant members of staff are also suitably trained as 'Applicants'.

An authorisation must not be approved until the Authorised Officer is satisfied that the activity proposed is necessary and proportionate.

- **Necessary** 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,
- 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,

Authorised Officers must pay particular attention to Health & Safety issues that may be raised by any proposed surveillance activity. Approval must not be given until such time as any health and safety issue has been addressed and/or the risks identified are minimised.

Authorised Officers must ensure that staff who report to them follow this document and do not undertake any form of surveillance, or access communications data, without first obtaining the relevant authorisation in compliance with this document.

Authorised Officers must ensure when sending copies of any forms to the Head of Trading Standards for inclusion in the Central Register, that they are sent in **sealed** envelopes and marked **Strictly Private & Confidential**.

General Information on RIPA

The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law) requires the City Council, and organisations working on its behalf, to respect the private and family life of citizens, his home and his correspondence.

The European Convention did not make this an absolute right, but a qualified right. Therefore, in certain circumstances, the City Council may interfere in an individual's right as mentioned above, if that interference is:-

(a) **In accordance with the law;**
(b) **Necessary**; and
(c) **Proportionate**.

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS')** – e.g. undercover agents, and **Accessing Communications data**. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

Directly employed Council staff and external agencies working for the City Council are covered by the Act for the time they are working for the City Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by two Authorised Officers.

A list of officers who may authorise Directed Surveillance is kept by the Head of Trading Standards. For the purposes of Accessing Communications Data the Designated Persons are the Head of Trading Standards and Head of Operations, Public Safety.

If the correct procedures are not followed, evidence may be dis-allowed by the courts, a complaint of mal-administration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the City Council and will, undoubtedly, be the subject of adverse press and media interest.

A flowchart of the procedures to be followed appears at **Appendix 1**.

What RIPA Does and Does Not Do

RIPA does:

- Requires prior authorisation of directed surveillance
- Prohibits the Council from carrying out intrusive surveillance
- Requires authorisation of the conduct and use of a CHIS
- Require safeguards for the conduct and use of a CHIS
- Requires proper authorisation to obtain communication data
- Prohibits the Council from accessing 'traffic data'

RIPA does not:

- Make unlawful conduct which is otherwise lawful
- Prejudice or dis-apply any existing powers available to the City Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

  If the Authorised Officer or any Applicant is in any doubt, they should ask the Head of Trading Standards before any directed surveillance, CHIS, or Access to Communications is authorised, renewed, cancelled or rejected.

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).

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.

Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

For the avoidance of doubt, only those Officers designated as 'Authorised Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, from 1 January 2004, are followed.

Intrusive Surveillance

This is when it: -

- Is covert;
- Relates to residential premises and private vehicles; and
- Involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Only police and other law enforcement agencies can carry out this form of surveillance.

Council Officers must not carry out intrusive surveillance.

Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	▪ Police Officer or Parks Warden on patrol ▪ Sign-posted Town Centre CCTV cameras (in normal use) ▪ Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. ▪ Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	▪ CCTV cameras providing general traffic, crime or public safety information.
Directed (must be RIPA authorised)	▪ Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. ▪ Test purchases where the officer has a hidden camera or other recording device to record information that might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive	▪ Planting a listening or other device (bug) in a person's home or in their private vehicle.

Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

A Covert Human Intelligence Source (CHIS) is someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain Information.

A member of the public who volunteers information to the City Council as part of their normal civic duties, or to contact numbers set up to receive information is not a CHIS.

What must be authorised?

The Conduct or Use of a CHIS require prior authorisation.

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
- **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive or their Deputy may authorise the use of Juvenile Sources.

Vulnerable Individuals

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive or their Deputy may authorise the use of Vulnerable Individuals.

Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

Anti-social behaviour activities (e.g. noise, violence, racial harassment etc)

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues.

Placing a covert stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

Accessing Communications Data

Local authority employees (except Housing Benefit Officers) will no longer be able to use their powers under relevant legislation and the exemption under the Data Protection Act 1998. The disclosure of communications data 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 the 'Designated person'.

Authorities are required to nominate Single Point of Contacts and that person(s) must have undertaken accredited training.

'Designated Persons' should hold a position within the local authority equivalent to or above Assistant Chief Officer, Head of Service or Service Manager.

Local authorities may only access to 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**. Local authorities do not have access to this data.**

Authorisation Procedures

Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

Authorised Officers

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire.

The authorisations do not lapse with time!

Authorised Officers–Access to Communications data

The Head of Trading Standards and Head of Operations, Public Safety are the 'Designated persons' permitted to authorise the obtaining and disclosing of communications data. The Head of Trading Standards also acts as the Single Point of Contact. Where an application is made from within Trading Standards, the Designated Person will always be the Head of Operations

Training Records

A certificate of attendance will be given to anyone undertaking training. Training will be recorded on their individual learning and development plan.

Single Points of Contact under Part 1 are required to undertake accredited training. A record will be kept of this training and any updating.

Grounds for Authorisation

Directed Surveillance or the Conduct and Use of the CHIS and Access to Communications Data can be authorised by the City Council only on one of the following grounds

- For the prevention or detection of crime or disorder

Assessing the Application Form

Before an Authorised Officer signs a Form, **they must**

Be mindful of this Corporate Policy & Procedures Document

Satisfy themselves that the RIPA authorisation is i**n accordance with the law, is Necessary, and Proportionate**

This means that they must establish whether other less invasive methods to obtain the information has been considered and balance the right of privacy against the seriousness of the offence under investigation.

Take account of the risk of intrusion into the privacy of persons other then the specified subject of the surveillance **(Collateral Intrusion).**

Ensure that measures are taken wherever practicable to avoid or minimise collateral intrusion.

Set a date for review of the authorisation and review on only that date.

Allocate a Unique Reference Number (URN) for the application.

Maintain a Departmental Register, and copy the relevant form (and any review/cancellation of the same) is forwarded to the Head of Trading Standards within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorised Officer **must also**

Be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

Consider the likely degree of intrusion of all those potentially affected;

Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

Ensure **records** contain particulars and are not available except on a need to know basis

.

Urgent Authorisations

In exceptional circumstances urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.

It will not be urgent where the need for authorisation has been neglected or is of the officer's own making.

It is policy that two officers authorise directed surveillance, however when an authorisation meets the above criteria then it is permissible for one officer to give oral authorisation. The authorising officer must make a record of the authorisation.

Urgent authorisations should last for no more than 72 hours. They must be recorded in writing on the standard form as soon as practicable and include an explanation of why the authorisation was urgent.

Duration

The Form **must be reviewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to conduct the surveillance lasts for a maximum of 3 months for Directed Surveillance and 12 months for a Covert Human Intelligence Source. In respect of a notice or authorisation to obtain communications data the period is one month.

Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

The renewal will begin on the day when the authorisation would have expired.

Working With Other Agencies

If an officer wishes to utilise the CCTV system operated by the Police Directed Surveillance Authorisation must be obtained before an approach is made to the Control Room. If immediate action is required an Authorisation must be obtained within 72 hours of the request being made.

When some other agency has been instructed on behalf of the City Council to undertake any action under RIPA, this Document and the Forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When another Enforcement Agency (e.g. Police, Customs & Excise, Inland Revenue etc): -

Wish to use the City Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures. Before any Officer agrees to allow the City Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form, or written confirmation that a Directed Surveillance Authorisation is in place.

Wish to use the City Council's premises for their own RIPA action, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the City Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the City Council's co-operation in the agent's RIPA operation. In such cases, however, the City Council's own RIPA forms should not be used as the City Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

Record Management

A Central Register of all Authorisation Forms will be maintained and monitored by the Head of Trading Standards.

Records maintained in the Department

- A copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorised Officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation, together with supporting
- Documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the Authorised Officer;
- The Unique Reference Number for the authorisation (URN).

Central Register maintained by Trading Standards

Authorised Officers must forward details of each Form to Trading Standards for the Central Register, **within 1 week of the authorisation, review, renewal, cancellation or rejection**.

Records will be retained records for three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) and the Interception Commissioner can audit/review the City Council's policies and procedures, and individual authorisations.

Concluding Remarks

Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure may be that the action (and the evidence obtained), is held to be inadmissible by the Courts pursuant to Section 6 of the Human Rights Act 1998.

Obtaining an authorisation under RIPA and following this document will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

Authorised Officers should be suitably competent and must exercise their minds every time they are asked to sign the request. They must never sign or rubber stamp Form(s) without thinking about their personal and the City Council's responsibilities.

Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

For further advice and assistance on RIPA, please contact the Head of Trading Standards. **(Extension 2486)**

DIRECTED SURVEILLANCE

Form A1 – Application for authorisation

Form A2 – Authorisation

Form A3 – Review

Form A4 – Renewal

Form A5 – Cancellation

Covert Human Intelligence Sources (CHIS)

Form B1 – Application for authorisation

Form B2 – Renewal

Form B3 – Review

Form B4 – Cancellation

Access to Communications Data

Form C1 – Application to obtain communications data

Form C2 – Cancellation

Form C3 – SPOC Log Sheet

Form C4 – SPOC Rejection Form

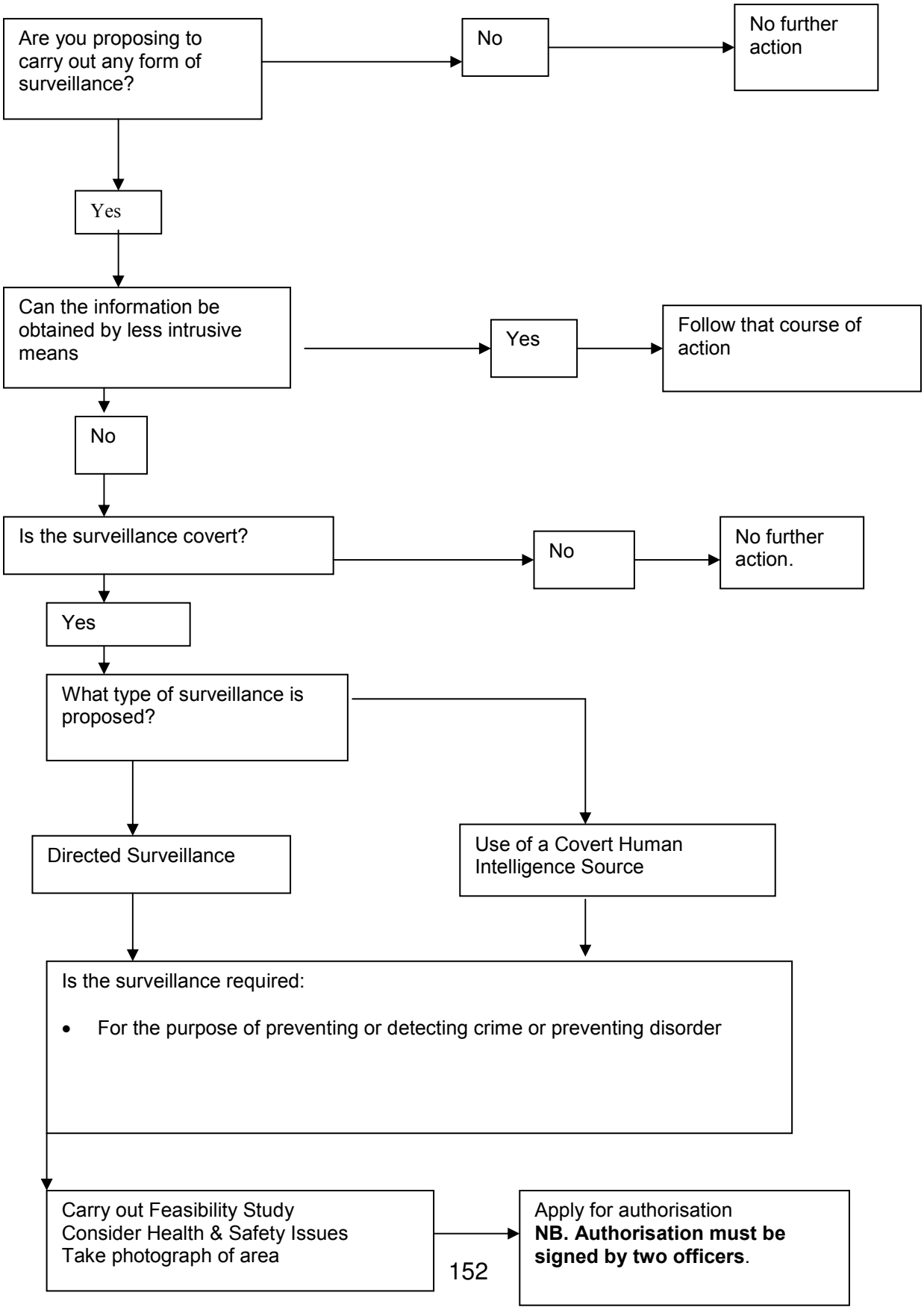
Form C5 – SPOC report

Form C6 – Designated Person Considerations

Forms can be obtained from the Head of Trading Standards or accessed via The Wave.

Appendix 1

Surveillance Activity Decision Process



Authorising Directed Surveillance Process Map