COVERT SURVEILLANCE

COUNCIL PROCEDURES

CONTENTS

1. Introduction
2. Benefits of Obtaining Authorisation
3. Directed Surveillance
4. Covert Human Intelligence Sources
5. Authorisation Process
6. Confidential Material
7. Joint Operations
8. Communications Data
9. Handling & Disclosure of Product
10. Use of Electronic Surveillance Devices
11. Covert Surveillance of Social Networking Sites
12. Codes of Practice
13. Scrutiny & Tribunal

Appendix 1 – List of Authorising Officers

Appendix 2 – Use of Social Media

Appendix 3 – Mock Application

Section 1 – Introduction

1. Local Authorities powers to conduct covert surveillance come from the provisions of the Local Government Act 1972. The main restrictions on the use of those powers can be found in the Human Rights Act 1998, and in particular Article 8 of the European Convention on Human Rights (The right to respect for a person's private and family life).

2. The Regulation of Investigatory Powers Act 2000 (RIPA) (as amended) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected whilst also ensuring that law enforcement and security agencies can still exercise the powers they need to do their job effectively.

3. Covert surveillance carried out for reasons other than the investigation of qualifying criminal offences falls outside the scope of RIPA. Such surveillance can still be lawful, but extra care is needed to ensure such surveillance does not breach an individual's Human Rights.

4. Regard has been had to the Codes of Practice issued by the Home Office, in preparing these procedures.

5. All covert surveillance activity carried out by or on behalf of the Council **MUST** be authorised one of the properly trained Authorising Officers listed in Appendix 1 unless the activity has been lawfully authorised under another statutory provision and the Council's Monitoring Officer has confirmed that no authorisation is therefore required in accordance with this procedure document.

6. Individual Investigating Officers and Authorising Officers should familiarise themselves with this procedure document and the Codes of Practice issued by the Home Office.

7. Deciding when an authorisation is required is a question of judgement. However, if an investigating officer is in any doubt, he/she should immediately seek legal advice. **As a basic rule however, it is always safer to seek the appropriate authorisation.**

8. The Senior Officer within the Council with strategic responsibility for covert surveillance issues is Linda Rees-Jones, Head of Administration & Law

9. The 'Gate-keeping' Officer, with responsibility for vetting all covert surveillance applications and maintaining the Central Register is Robert Edgecombe, Legal Services Manager.

10. The elected member responsible for reviewing the authority's use of covert surveillance is Councillor Linda Evans.

SECTION 2 - BENEFITS OF OBTAINING AUTHORISATION UNDER RIPA

1. Where an authorisation is not obtained, there is a risk that any evidence obtained as a result could be ruled as inadmissible in subsequent legal proceedings.

2. Furthermore, unauthorised covert surveillance activity is more likely to result in a breach of an individual's human rights, leading to a compensation claim against the Council.

SECTION 3 - DIRECTED SURVEILLANCE

1. Directed Surveillance includes;

- The monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication.

- The recording of anything so monitored observed or listened to in the course of surveillance.

- The surveillance by or with the assistance of a surveillance device.

2. Directed Surveillance does NOT occur where covert recording of suspected noise nuisance takes place and the recording device is calibrated to record only excessive noise levels.

3. Directed Surveillance occurs if it is undertaken;

- For the purposes of a specific investigation or operation

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

OFFICERS SHOULD NOTE THAT THE SURVEILLANCE OF AN INDIVIDUAL'S ACTIVITIES AND/OR CONVERSATIONS IN *A* PUBLIC

PLACE MAY STILL AMOUNT TO THE OBTAINING OF PRIVATE INFORMATION

4. Surveillance is 'covert' if it is carried out in a manner calculated to ensure that the target is unaware it is or may be taking place. Therefore surveillance of an individual using overt CCTV cameras could still require authorisation if the cameras are targeted on that individual and he/she is unaware that they are being watched.

5. Directed surveillance becomes 'intrusive' if;

- It is carried out in relation to anything taking place on any residential premises or in any private vehicle, and

- Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device on the premises/vehicle, or

- Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being on the premises or vehicle, where the device is such that it 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 vehicle.

THE COUNCIL HAS NO POWER TO AUTHORISE INTRUSIVE SURVEILLANCE. IF INVESTIGATING OFFICERS HAVE ANY CONCERNS REGARDING THIS THEY SHOULD IMMEDIATELY SEEK LEGAL ADVICE.

6. Surveillance is for the purposes of a specific investigation or operation if it is targeted in a pre-planned way at an individual or group of individuals, or a particular location or series of locations.

7. Surveillance will not require authorisation if it is by way of an immediate response to an event or circumstances where it is not reasonably practicable to get an authorisation.

SECTION 4 - COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

1. A person is a CHIS 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 paragraphs immediately below.
- He/she covertly uses such a relationship to obtain information or 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.

2. A purpose is covert in this context if the relationship is conducted in a manner that is calculated to ensure that one of the parties is unaware of that purpose.

3. Council policy is to treat all such activities as being in need of authorisation whether or not the information sought is private information.

4. When considering whether to make use of CHIS, investigating officers ***MUST*** consult with the gate-keeping officer before taking any action, in order to ensure that the relevant Home Office Code of Practice is complied with. Where use is made of CHIS, his/her designated handler must be a properly trained officer, who may not necessarily be based within the same department/section as the investigating officer.

ONLY THE CHIEF EXECUTIVE MAY AUTHORISE THE USE OF A JUVENILE CHIS.

IT IS THE POLICY OF THIS AUTHORITY TO DISCOURAGE THE USE OF COVERT HUAN INTELLIGENCE SOURCES. THE AUTHORITY WILL ONLY DEPART FROM THIS POLICY IN THE MOST EXECEPTIONAL OF CIRCUMSTANCES

SECTION 5 - AUTHORISATION PROCESS

1. Applications must be in writing, using the standard forms

2. Although it is possible to combine two or more applications in the same form, this practice is generally to be avoided. One situation where it may be appropriate is during a covert test purchase exercise involving more than one premise. In such cases investigating officers should contact the gate-keeping officer to discuss the operation before completing the forms.

3. The application form must set out in detail:

   (a) What information it is hoped the surveillance will obtain
   (b) Why that information is essential to the investigation
   (c) What steps have already been taken to obtain that information

   A sample application is attached to this document at Appendix 3

4. Once the appropriate application forms are completed, they should be submitted by email to the gate-keeping officer.

5. The gate-keeping officer will then vet the application, enter it onto the Central Register and allocate a unique central reference number.

6. The gate-keeping officer may recommend changes to the application, or agree to it being submitted unaltered to a designated authorising officer.

7. Where an application must be authorised by the Chief Executive (ie in cases of a juvenile CHIS or confidential information), the gate-keeping officer will arrange a meeting between the investigating officer, gate-keeping officer and Chief Executive.

8. In all other cases the investigating officer shall arrange to meet one of the authorising officers to discuss the application.

9. When determining whether or not to grant an authorisation, Authorising Officers must have regard to;

- Whether what is proposed is necessary for preventing/detecting criminal offences that meet the requirements in Section 1 paragraphs 11 and 12 above.
- Whether what is proposed is proportionate to the aim of the action
- Whether the proposed action is likely to result in collateral intrusion into the private lives of third parties, and if it is, whether all reasonable steps are being taken to minimise that risk.
- In the case of applications to authorise the use of a CHIS, whether all the requirements of the Code of Practice relating to the authorisation of a CHIS issued by the Home Office are complied with.

10. If an application is refused, the reasons for refusal shall be endorsed on the application

11. If an application is granted, the authorising officer must specify;

- The scope of the authorisation
- The duration of the authorisation
- The date (not more than 28 days) for review of the authorisation.

12. Irrespective of the outcome of the application, the investigating officer must immediately forward a copy of the authorisation or refused application, to the gate-keeping officer, who will make the appropriate entries in the Central Register, and place the copy application or authorisation in the Central Record.

13. Where appropriate the gate – keeping officer will then arrange for an application to be made to the Magistrates Court for the judicial approval of the authorisation.

ALL OFFICERS MUST NOTE THAT AN AUTHORISATION REQUIRING JUDICIAL APPROVAL WILL NOT TAKE EFFECT UNTIL IT HAS BEEN JUDICIALLY APPROVED.

14. If, upon initial review of the authorisation, the authorising officer determines that it should remain in effect, reviews must take place every 28 days during the life of the authorisation. The investigating officer must keep a record the results of any review and communicate them to the gate-keeping officer for entry in the Central Register.

15. Once an authorising officer determines that an authorisation is no longer necessary it must be cancelled immediately.

16. Once the operation to which the authorisation relates is concluded, or the activity authorised ceases, then the investigating officer must immediately meet the authorising officer to cancel the authorisation.

17. Whenever an authorisation is cancelled, the authorising officer must endorse the cancellation with his/her views as to the value of the authorised activity.

18. Whenever an authorisation is cancelled, a copy of that cancellation must be sent to the gate-keeping officer for it to be placed in the Central Record, and appropriate entries to be made in the Central Register.

19. Unless previously cancelled, an authorisation will last as follows;

- Written authorisation for Directed Surveillance – **3 months**
- Written authorisation for use of a CHIS – **12 months**

20. If shortly before an authorisation ceases to have effect, the authorising officer is satisfied that the grounds for renewing the authorisation are met, then he/she may renew the authorisation. ***(Before renewing an authorisation, authorising officers must have regard to the appropriate sections of the relevant code of practice issued by the Home Office)***

21. An authorisation may be renewed for;

- In the case of a written renewal of a Directed Surveillance authorisation - **3 Months**.
- In the case of a written renewal of a CHIS authorisation – **12 months**.

22. An authorisation may be renewed more than once.

23. Applications for renewal of an authorisation must record all matters required by the relevant Code of Practice issued by the Home Office

24. Where an authorisation is renewed, it must continue to be reviewed in accordance with the requirements set out above.

25. Where an authorisation is renewed, a copy of the renewal must be sent to the gate-keeping officer and placed in the Central Record and appropriate entries made in the Central Register.

26. Where appropriate the gate-keeping officer will then arrange for an application to be made to the local magistrates' court for the judicial approval of the renewal.

ALL OFFICERS MUST NOTE THAT WHERE A RENEWAL REQUIRES JUDICIAL APPROVAL IT WILL NOT TAKE EFFECT UNTIL IT HAS BEEN JUDICIALLY APPROVED.

WHERE AN APPLICATION IS GRANTED OR RENEWED THE INVESTIGATING OFFICER MUST ENSURE THAT ALL OFFICERS TAKING PART IN THE COVERT SURVEILLANCE ACTIVITY HAVE AN OPPORTUNITY TO READ THE AUTHORISATION AND FAMILIARISE THEMSELVES WITH ITS TERMS AND RESTRICTIONS BEFORE THE OPERATION COMMENCES.

SECTION 6 - CONFIDENTIAL MATERIAL

1. Confidential material such as;
   (i) personal medical information
   (ii) spiritual information,
   (iii) confidential journalistic information
   (iv) information subject to legal privilege

This Information is particularly sensitive and is subject to additional safeguards.

2. In cases where such information may be obtained, an investigator must seek immediate legal advice.

3. **Only the Chief Executive may authorise surveillance activity which may result in confidential information being obtained.**

4. Any application for an authorisation, which is likely to result in the acquisition of confidential material MUST include an assessment of how likely it is that confidential material will be acquired.

5. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances and with full regard to the proportionality issues this raises.

6. The following general principles apply to confidential material acquired under such authorisations;

- Officers handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is any doubt, immediate legal advice should be sought.
- Confidential material should not be retained or copied unless it is necessary for a specified purpose.
- Confidential material should only be disseminated, after legal advice has been sought, where it is necessary for a specified purpose.
- The retention and/or dissemination of confidential material should be accompanied by a clear warning of its confidential nature.
- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

SECTION 7 - JOINT OPERATIONS

1. Where officers are engaged in operations with other public authorities, any covert activity must be authorised either in accordance with this document, or by an appropriate officer employed by the other authority.

2. Officers should always ensure that when operating under an authorisation issued by another authority, that the authorising officer has the power to issue that authorisation, and that the authorisation covers the scope of the proposed activity.

3. Officers are advised to request a copy of the relevant authorisation, or at least obtain a written note of the scope, duration and conditions of the authorised activity.

4. Officers should also have regard to any other protocols specifically dealing with joint operations.

SECTION 8 – COMMUNICATIONS DATA

1. Local authorities have no power to covertly intercept communications between third parties such as letters, text messages and telephone calls.

2. However, local authorities do have the power to give notice or seek authorisation to obtain certain types of postal and communications data such as who a particular telephone number is registered to or whether someone has asked for their mail to be diverted to another address.

3. The process for seeking such authorisations is now covered by Section 60A of the Investigatory Powers Act 2016

4. In summary, any request to access communications data must me made by the National Anti-Fraud Network (NAFN) to the Investigatory Powers Commissioners Office (IPCO) on behalf of the Council.

5. **Officers wishing to acquire communications data under this procedure should discuss their plans with the the 'Gate-Keeping' officer before approaching NAFN.**

SECTION 9 - HANDLING & DISCLOSURE OF PRODUCT

1. Officers are reminded of the rules relating to the retention and destruction of confidential material set out in the relevant section above.

2. Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material.

3. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of such an investigation, and there is no reason to believe it will be relevant to future criminal or civil proceedings, it should be destroyed immediately.

4. Consideration as to whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

5. The law does not prevent material properly obtained in one investigation being used in another investigation. **However, the use of any covertly obtained material for purposes other than that for which the surveillance was authorised should only be sanctioned in exceptional cases and only after seeking legal advice.**

SECTION 10 - USE OF SURVEILLANCE DEVICES

1. Surveillance devices include, static and mobile CCTV cameras, covert surveillance cameras, noise monitoring/recording devices, and any other mechanical and/or recording devices used for surveillance purposes.

2. Fixed security cameras, which are incapable of being remotely controlled, do not require RIPA authorisation ***provided*** their existence and purpose is made clear to the public through appropriate signage. The use of these cameras is governed by separate requirements regulated by the Surveillance Camera Commissioner.

3. Overt ‘fixed’ CCTV cameras will not ordinarily require authorisation where their existence and use is also made clear by signage. However, where officers with responsibility for such systems are requested to allow the police (or other similar organisations) the view camera footage in real time for the purpose of targeting specific individuals, then the following rules apply;

- Where the request is made by way of an immediate response to an incident or intelligence received, no authorisation is required, subject to the requirements below.
- Where the request is made as part of a pre-planned operation or investigation, the Officer with responsibility for the CCTV system in question should ask to see the RIPA authorisation (or a summary of it) before any surveillance takes place.

4. It is recognised that many departments maintain conventional cameras and mobile phone cameras for use by staff on a regular basis. Staff must be reminded;

- That the covert use of such cameras (ie where the ‘target’ is not aware that he/she is being photographed) may require authorisation.
- As a general rule, unless a covert photograph is being taken as an immediate response to an unexpected incident, authorisation should be sought.

5. Use of noise monitoring/recording equipment may also require authorisation, where the equipment records actual noise, as opposed to just noise levels. Much will depend upon what noise it is intended, or likely, to record.

6. Where a target is made aware in writing that noise monitoring will be taking place, then authorisation is not required.

7. Service Managers with responsibility for surveillance devices **MUST** ensure that;

   (i) Those devices are stored securely and that robust systems are in place to prevent unauthorised access to them both by Council staff and members of the public.
   (ii) Full and accurate records are kept at all times documenting the use of those devices including (but not limited to), when deployed, the purpose of any deployment, the officer with responsibility for that deployment and, where being deployed to conduct Directed Surveillance, details of any authorisation under which that deployment takes place.
   (iii) Any personal information obtained as a result of the deployment of such a device is handled in accordance with the Council’s Data Protection Policies.

SECTION 11 – COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

1. Care must be taken when using or monitoring a social networking site for work purposes. Even though a site may seem to be an open source of publically available information, the author may have expectations of privacy, especially if they apply at least some access controls.

2. The use of a false identity on a social networking site for this purpose is permissible, but is likely to require authorisation under the terms of this document.

3. If the monitoring of a social networking site is proposed which involves getting past access or privacy controls without the author of the site knowing that it is a public authority that is trying to gain access, then it is likely that covert surveillance is taking place which interferes with that persons human rights and authorisation will be required.

4. Any use of a Social Networking site for these purposes must also comply with Council policies on Internet and Social Media Usage.

5. ONLY THE COUNCIL'S MEDIA AND MARKETING TEAM MAY CREATE FALSE SOCIAL MEDIA PROFILES FOR USE BY COUNCIL STAFF

6. **UNDER NO CIRCUMSTANCES SHOULD COUNCIL STAFF USE THEIR PERSONAL SOCIAL MEDIA PROFILES TO CONDUCT ANY FORM OF SURVEILLANCE FOR WORK PURPOSES.**

7. For more information regarding online surveillance activity see Appendix 2

SECTION 12 - CODES OF PRACTICE

1. The Home Office has issued Codes of Practice relating both to Directed Surveillance and the use of CHIS. Copies of these codes are available via the Home Office website.

2. Whilst these codes do not have the force of law, they represent best practice, and adherence to them will give the authority a better chance of opposing any allegation that RIPA and/or the Human Rights Act has been breached.

3. Investigating and Authorising Officers should ensure that when dealing with applications, regard is had to these codes.

SECTION 13 - SCRUNTINY AND TRIBUNAL

The council will be subject to an inspection by an Investigatory Powers Commissioners Office (IPCO) inspector roughly every 2 years. The inspector may;

- Examine the Central Register
- Examine authorisations, renewals and cancellations
- Question officers regarding their implementation of the legislation.
- Report to the Chief Executive regarding his/her findings

A Tribunal has also been set up to deal with complaints made under RIPA. The tribunal may quash or cancel any authorisation and order the destruction of any record or information obtained as a result of such an authorisation.

Courts and Tribunals may exclude evidence obtained in breach of an individual's human rights. Failure to follow the procedures set out in this document increases the risk of this happening.

This document will be kept under review by the relevant Cabinet Member.

APPENDIX 1 – LIST OF AUTHORISING OFFICERS UNDER THE REGULATION OF INVESTIGATING POWERS ACT

Name	Post
Wendy Walters	Chief Executive
Ainsley Williams	Director of Environment
Sue E Watts	Environmental Protection Manager